
Mit Stellenmarkt
iX
Anzeige
+++ NEU: Inklusiv-Traffic verdoppelt! +++ Große Sparaktion! +++
NaturEnergie 100 % CO2 FREI
STRATO V-PowerServer
www.strato.de
siehe Seite 4 + 5
MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK
7 Juli 2008
€ 5,50 H 10554
Auf der Heft-CD:
• 22 × Blog-Software zum Ausprobieren
• XAMPP – Apache, MySQL, PHP, Perl startfertig für Windows
IT-Security:
Kreditkarten im Visier
WLAN-Zugang im Griff
Tutorial:
Ruby on Rails
Registrierung, Bilder
Schreiben und schreiben lassen:
Blog-Software
Vergleichstests Weblog-Pakete, Mikro-Blogging mit Twitter
Embedded Systems:
MDA mit Eclipse
Linux-kompatibler geworden:
FreeBSD 7.0
Eclipse-Alternative:
Netbeans 6
Interaktives Web:
Social Network APIs
Geschäftsmodelle:
Geld verdienen mit Open Source
Mobilität nach Maß:
Blackberry-Programme entwickeln
Von DB2 bis Sybase:
Tools fürs Datenbankmanagement
Liebes Tagebuch, heute ist mein Notebook angekommen, und jetzt kann ich endlich bloggen.
Datenträger enthält Info- und Lehrprogramme gemäß § 14 JuSchG
4 199148 505501 07
Juli 2008 www.ix.de iX Magazin für professionelle Informationstechnik
Österreich € 6,20 Schweiz CHF 10,70 Benelux € 6,70 Italien € 6,70
Heise

# Schluss mit lustig

Fünf Euro pro Tag betrug die Teilnahmegebühr für das erste deutsche Wardriver-Treffen, das im Februar 2003 in Berlin stattfand. Zum Programm gehörten ein Workshop zum Antennenselbstbau und zur Bedienung der Wardriving-Software sowie eine Tour durch die Stadt – „natürlich mit entsprechendem Equipment zum Scannen der Wireless-Netzwerke“, was heise online damals als quasi selbstverständlich meldete.

Dabei sind Wardriver-Treffen nichts anderes als Verabredungen zu Straftaten, ein Antennenbau-Workshop eine Anleitung zum Abhören von Nachrichten. So sieht es zumindest das Wuppertaler Amtsgericht in einem bereits im April vorigen Jahres gefällten, aber erst kürzlich veröffentlichten Urteil (Az. 22 Ds 70 Js 6906/06).

Zwar wurde der Angeklagte, der einen nachbarlichen Access Point ohne zu fragen als Internetzugang genutzt hatte, nur verwarnt. Erst im Wiederholungsfall drohen ihm 20 Tagessätze. Denn, so das Gericht, die Rechtlage für solche Fälle sei ja „bislang ungeklärt“ gewesen. Doch das Tatwerkzeug, sein Laptop, wurde eingezogen.

Die Urteilsbegründung wirkt auf Nicht-Juristen, gelinde gesagt, streckenweise praxisfern. Die vom WLAN-Router zugewiesene IP-Adresse gilt dem Gericht als abgehörte Nachricht, da sie nicht für den Angeklagten bestimmt war. Zudem sei eine IP-Adresse ein personenbezogenes Datum, sodass auch ein Verstoß gegen das Bundesdatenschutzgesetz vorliege.

Auch wenn man Letzteres prinzipiell gutheißen mag, weil sich daraus die Vertraulichkeit der IP-Adresse etwa gegenüber Herausgabeansinnen von Sicherheitsbehörden und Medienindustrie ableiten lässt – in diesem Fall hatte ja eben nicht der Angeklagte die IP-Adresse des vermeintlich Geschädigten ausgespäht, sondern selbst eine zugewiesen bekommen. Dass es sich dabei um eine Adresse aus einem der privaten, nicht an spezielle Inhaber vergebenen IP-Adressbereiche gehandelt haben dürfte, macht das Ganze vollends absurd.

Und wie soll in der Logik des Wuppertaler Urteils ein Fall gewertet werden, bei dem sich ohne Zutun des Benutzers sein Rechner mit dem nächsterreichbaren WLAN verbindet? Will man auch dem unerfahrenen User eine aktive Prüfungspflicht aufbürden?

Fragen, die sich dem Gericht wahrscheinlich nicht gestellt haben. Leider liegt die Vermutung nahe, dass der Grund dafür wieder einmal technische Unbedarftheit war. Denn derartige Urteile haben alles andere als Seltenheitswert.

Hätte sich der Wuppertaler Richter nämlich mit der Frage befasst, welche Verhaltensweisen spürbar negative Folgen nach sich ziehen, hätte er den Betreiber des offenen WLAN verurteilt. Denn der hat durch mangelnde Sicherheitsvorkehrungen sein Rechnernetz für illegale Aktivitäten nahezu jeder Art zur Verfügung gestellt, von der Vorbereitung von DDOS-Angriffen über die Installation einer Spam-Schleuder bis zur Verbreitung von Kinderpornografie.

Damit soll nicht der strafrechtlichen Verfolgung von unbedarften Computer-Hobbyisten das Wort geredet werden. Doch naheliegender als die Bestrafung folgenlosen Wardrivens wäre sie allemal.

Jürgen Seeger

JÜRGEN SEEGER



iX-Link ix0807003

Juli 2008



## Gründlich überholt: FreeBSD 7.0



Das Feeling „Von Programmierern für Programmierer“ konnten die BSD-Unixe nie ganz ablegen. Dass das kein Nachteil sein muss, zeigt das immer Linux-verträglichere FreeBSD 7.0.

Seite 68

## WLAN-Eindringlinge aufspüren

Das Aufspüren ungebetener WLAN-Gäste per „Warwalking“ artet vor allem bei großen Installationen schnell zur Sisyphos-Arbeit aus. Als effektiver haben sich Verfahren erwiesen, die Eindringlinge über das LAN suchen.

Seite 100




Die meisten Unternehmen nutzen nicht nur die Datenbank eines Herstellers. Dass das nicht zwangsläufig zum Tool-Wirrwarr auf dem Desktop des Administrators führen muss, zeigt unsere Marktübersicht zu RDBMS-übergreifenden Verwaltungswerkzeugen.

Seite 94




# Mit CD: Freie Blog-Software

Blogs beziehungsweise Weblogs haben sich zur Verbreitung von Nachrichten und Meinungen „von unten“ schnell etabliert. Die Auswahl an entsprechender Software ist groß, die meiste frei verfügbar. Ein exemplarischer Vergleichstest, eine Auswahl von 22 Softwarepaketen auf CD und ein Blick über den Tellerrand auf Twitter.

Seiten 42 und 54



# Embedded MDA mit Eclipse

Auch für eingebettete Systeme bietet modellgetriebene Softwareentwicklung eine Reihe von Vorteilen. Wie sich dies in einer Eclipse-basierten Werkzeugkette darstellt, demonstriert eine Ampelsteuerung.

Seite 116



## Nicht ganz so restriktiv

(Linux SBS: Arbeitspferde für kleinere Unternehmen; *iX* 6/08; S. 48)

Beim Überfliegen des Artikels „Linux en miniature“ ist mir auf Seite 49 ein, meiner Meinung nach, größerer Fehler aufgefallen. Dort steht in der linken Zeile im 2. Absatz: „Der Zusatz „Small Business“ ist durchaus ernst zu nehmen: Mehr als 75 Client-Lizenzen sind nicht vorgesehen, ebenso wenig wie weitere Windows-Server im Netz.“

Dieser Satz stimmt bis zu den Client-Lizenzen. **Aber:** Natürlich dürfen im Netz mehrere Windows-Server stehen. Der SBS ist „lediglich“ darauf beschränkt, der primäre Domänen-Controller sein zu müssen! Weitere Domänen-Controller müssen ihm untergeordnet sein. Alle anderen Windows-Server, die keine AD-Server sind, können sich zu Massen im Netzwerk tummeln.

STEFAN KELLERMANN, VIA E-MAIL






*Der Leser hat Recht. Richtig hätte es heißen müssen: „… ebenso wenig wie weitere SBS-Server respektive andere AD-Controller im Netz.“ (d. Red.)*

## Faszinierend …

(Editorial: Die Komplexitätsfalle; *iX* 6/08; S. 3)

Faszinierend finde ich, dass vieles früher problemlos geklappt hat. Bei uns haben wir bisher mit Cobol, Cics und DB2 auf dem Großrechner gearbeitet. Alle Unterprogramme haben sich ohne weiteres gefunden und ließen sich mit minimalem Aufwand aufrufen.

Aber das ist ja Technologie von vorgestern. Heute machen wir das in Java, und da heißt es: XML ist wie Gewalt. Wenn XML nicht ausreicht, hast du nur nicht genug genommen. Was früher in einer einzigen Cobol-Datei untergebracht war, erfordert nun 20 *xml*- und *properties*-Dateien, Build-Skripte und dergleichen. Während früher eine Produktionsübergabe harmlos war und jederzeit ging, darf man das wegen des riesigen Aufwandes heute nur noch einmal im Quartal machen.

Der Aufwand ist derzeit dabei, von Faktor 10 auf Faktor 7 zu sinken. Aber was tut man nicht für den technischen Fortschritt und dafür, dass die User bunte Masken haben, die sich nicht mehr ohne Sehnenscheidenentzündung bedienen lassen.

PHILIPP SEEGER, HANNOVER



## Nicht einsteigergerecht

(Rails-Tutorial I: Einrichten und anpassen; *iX* 6/08; S. 124)

Ich begrüße, dass endlich eine professionelle Zeitschrift wie *iX* dem Ruby on Rails Web Framework ein dreiteiliges Tutorial widmet. Leider verpassen Sie größtenteils das Ziel, die Einstiegshürden in die wunderbare RoR-Welt zu senken – meistens durch fehlende und/oder fehlerhafte Listings. Das Tutorial setzt nämlich Kenntnisse voraus, die man nicht von einem Ruby-on-Rails-Anfänger verlangen kann: die (zu) kurze Einführung vom Konzept der „REST-

**DER DIREKTE DRAHT ZU *iX***

Direktwahl zur Redaktion: 05 11/53 52-387

Bitte entnehmen Sie Durchwahlnummern und E-Mail-Adressen dem Impressum.

| Redaktion iX<br>Postfach 61 04 07<br>30604 Hannover | Fax: 05 11/53 52-361<br>E-Mail: <user>@ix.de<br>Web: www.ix.de |
|---|---|

Sämtliche in *iX* seit 1990 veröffentlichten Listings sind über den iX-FTP-Server erhältlich: ftp.heise.de/pub/ix/

iX-Link Bei Artikeln mit diesem Hinweis können Sie auf www.ix.de das zugehörige Argument (ixJJMMSSS) eingeben, um eine klickbare Liste aller URLs zu bekommen.

ful Controller Actions“ und die Abwesenheit des „TrainspotsController“-Listings ermöglichen einem Neuling kaum, die von ihnen vorgestellte Beispiel-Applikation überhaupt zu verstehen und lauffähig umzusetzen.

Von einem Tutorial erwarte ich, dass ein unerfahrener Programmierer die Beispiel-Applikation wenigstens lauffähig programmieren kann … leider trifft das hier nicht zu. All denen, die das Thema „RESTful Controller Actions“ verstehen möchten, kann ich nur die Lektüre von „The Rails Way“ empfehlen (Autor: Obie Fernandez, Verlag: Addison Wesley Professional, ISBN-13: 978-0321445612): Insbesondere Kapitel 4 liefert eine verständliche Einführung in die Benutzung von *named routes*.

Nichtsdestotrotz: Die Initiative ist mehr als lobenswert, da Sie trotz Mängeln eine Einführung in das RoR Framework bieten – Mängel, die hoffentlich durch Teil 2 und 3 des Tutorials behoben werden, insbesondere durch mehr Leitfaden zu einer funktionsfähigen Umsetzung der Beispiel-Applikation.

SERGIO DA SILVA, LUXEMBURG

*Wahrscheinlich haben wir nicht deutlich genug darauf hingewiesen: Über den Listing-Service (ftp.heise.de/ix/) sind die kompletten, lauffähigen Listings verfügbar, die im Heft wurden aus Platzgründen gekürzt.* *(d. Red.)*



## Mit und ohne *cron*

(Web-CMS: Drupal 6 – Neue APIs und mehr Komfort; *iX* 5/08; S. 62)

Bei der *iX*-Wertung für Drupal 6 geben Sie einen Minuspunkt für „Drupal setzt Zugriff auf cron voraus“. Dazu möchte ich drei Dinge mitteilen: Erstens funktioniert das Drupal-Kern-System auch ohne Cron. Zweitens wird Drupal über eine PHP-Datei namens *cron.php* im Web-Verzeichnis aufgerufen. Dies erlaubt eine manuelle Ansteuerung durch einen Benutzer oder die Verwendung externer Cron-Routinen (z. B. mit Lynx). Auf diesem Weg lässt sich die Uptime einer Drupal-Website regelmäßig überprüfen. Drittens gibt es das Modul Poormanscron, das die Cron-Routine aufgrund von anderen Website-Aktivitäten – auch durch Website-Gäste – ansteuert (http://drupal.org/project/poormanscron).

CARSTEN LOGEMANN, FRANKFURT AM MAIN

## Unvollständige Mehrdeutigkeit

(Suchverfahren: Semantische Ansätze; *iX* 5/08; S. 118)

Das Beispiel „Police“ als Beispiel für semantische Mehrdeutigkeit ist sogar unvollständig geblieben, denn es gibt ja noch die Versicherungs-Police. Man sieht also, dass auch ein Mensch bei einem derart „einfachen“ Beispiel durchaus Fehler machen kann.

JÖRG MICHAEL, HANNOVER

## Unnötige Skriptmanipulation

(Webprogrammierung: Open-Source-Compiler für Actionscript; *iX* 6/06; S. 136)

Die im Artikel beschriebenen Manipulationen des Installationsskriptes *installFMS* sind vollkommen unnötig. Ein Blick in die Hilfe des Skriptes (*–help* oder *-usage*) offenbart den Parameter *-platformWarnOnly*, der die Installation auch auf nicht unterstützten Unix-Plattformen erlaubt. Damit ist mir die Installation sowohl unter Fedora 8 als auch unter der 64-Bit-Version von SuSe 10.1 gelungen.

INGO SCHAEFER, BRANDENBURG

## Ergänzungen und Berichtigungen

(XML: Herstellerunabhängiges Reporting mit XSL und Co.; *iX* 6/08; S. 106)

Im zweiten Satz muss es heißen „Die dadurch entstehende Herstellerabhängigkeit …“ statt „ … Herstellerunabhängigkeit …“.



Die *iX*-Redaktion behält sich Kürzungen und auszugsweise Wiedergabe der Leserbriefe vor. Die abgedruckten Zuschriften geben ausschließlich die Meinung des Einsenders wieder, nicht die der Redaktion.




## Mehrkerniger Hund

Texas Instruments (TI, www.ti.com) stellte sein Beagleboard (beagleboard.org) vor. Das 79 × 76 mm² kleine Board dient als freie Entwicklungsplattform für die primär in mobilen Geräten eingesetzte OMAP3-Familie. Basis ist ein TI OMAP3530, der aus einem ARM Cortex-A8 Core mit 600 MHz, einem Signalprozessor TMS320C64x mit 430 MHz und einer Imagination SGX 2D/3D GPU besteht. Es stehen 128 MByte DDR RAM und 256 MByte Flash sowie ein SD-Kartenslot zur Verfügung; die GPU arbeitet mit Shared Memory. Neben dem S-Video-Anschluss gibt es einen für HDMI, Stereo-Ein- sowie -Ausgang sind ebenfalls vorhanden. Den Anschluss an die Außenwelt realisieren ein RS232-Port sowie USB 2.0. Der Chip verfügt über zwei integrierte USB-Controller. Einer „spricht“ mit den Peripheriegeräten, wie Speichersticks, Webcam, WLAN-Karte et cetera, der Zweite fungiert als Peripheriegerät und erlaubt beispielsweise die Kommunikation mit einem PC. Über die 14-polige Jtag-Schnittstelle lässt sich der OMAP3530 debuggen und das Flash programmieren. Eigene Hardwareerweiterungen werden an eine 28-Pin-Pfostenleiste anschlossen, dort finden sich I2C, I2S, SPI und eine MMC/SD-Schnittstelle.

Sowohl für den ARM Cortex-A8 als auch für den DSP TMS320C64x benötigen Entwickler je einen Debbuger und Compiler. Diese und weitere benötigte Tools sind auf der Projektseite zum kostenlosen Download verlinkt. Neben dem Booten aus dem Flash unterstützt das nur knapp 150 US-Dollar kostende Board unter anderem das Starten via USB oder von SD-Karte.

*Axel Urbanski*



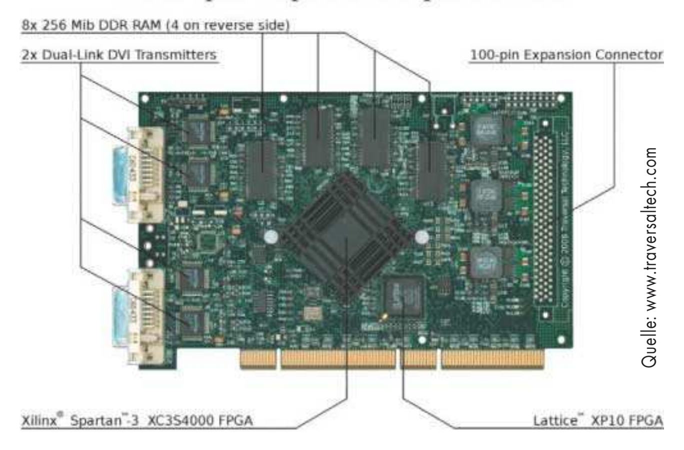

## Mehr als nur Grafik

Das Opengraphics-Team (wiki.opengraphics.org) nutzte den Linuxtag in Berlin, um seine komplett unter der GPL stehende Grafikkarte vorzustellen. Der Prototyp mit zwei DVI-Anschlüssen basiert auf einem Xilinx Spartan 3 XC3S4000 FPGA und verfügt über 256 MByte DDR RAM. Noch etwas ungewöhnlich ist der 64-Bit-PCI-X-Anschluss. Den Kontakt zwischen PCI-X und dem Spartan 3 übernimmt ein Lattice XP10 FPGA. Ein 100-poliger Erweiterungsanschluss für eigene Entwicklungen und Erweiterungen rundet das Bild ab. Die Karte soll im Mittel 20 Watt Leistung aufnehmen.

Nicht nur die Quellen der Treiber und der FPGA Firmware stehen zum Download auf der Website bereit, sondern auch Schaltpläne und Layouts des Boards. Es finden sich ebenfalls Links zu den freien Entwicklungstools der FPGA-Hersteller. Für die Vermarktung der Boards haben die Projektinitiatoren eigens die Firma Traversal Technology (www.traversaltech.com) gegründet.

*Axel Urbanski*

iX-Link ix0807010




Quelle: www.traversaltech.com

## Kolab-Client jenseits von Linux

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI, www.bsi.bund.de) zeigte auf dem Linuxtag Neues: Prototypen des KDE-PIM-Tools Kontact für Windows und Mac OS X, die in Zusammenarbeit mit dem Kolab-Projekt entstanden. Sie setzen nicht mehr auf Cygwin auf, sondern laufen als reine Qt-Programme nativ auf der jeweiligen Plattform. Ende des Jahres will das BSI die Portierung abgeschlossen haben und die neuen Clients nach Tests der Anwendungsszenarien freigeben.

Kontact ist (bis dato) ausschließlich der Linux-Client für den freien Groupware-Server Kolab (www.kolab.org), der selbst ebenfalls aus einem BSI-Projekt entstanden ist. Durch die Erweiterung der unterstützten Betriebssysteme bietet die Exchange-Alternative nun auch eigene Clients für bisher Outlook vorbehaltene Plattformen an. Die Möglichkeit der Outlook-Anbindung über proprietären Konnektoren für Kolab besteht natürlich weiterhin. Außerdem integrierten die Entwickler die Horde-Groupware (www.horde.org) für den webbasierten Zugriff in den Kolab-Server.

*Christian Böttger*




## Neue Version des Migrationsleitfadens

Die Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt, www.kbst.bund.de) hat ihren Migrationsleitfadens in der Version 3.0 vorgestellt. Diese aktualisiert die erstmals 2003 freigegebene Informationssammlung zu Softwaremigrationsprojekten in öffentlichen Verwaltungen. Darüber hinaus modularisierte die KBSt das Dokument in weitgehend unabhängige thematisch orientierte Module. Das soll einerseits die Lesbarkeit des rund 550 Seiten starken PDFs verbessern und andererseits sicherstellen, dass sich zukünftig einzelne Teile schneller aktualisieren und anpassen lassen. Im Gegensatz zu früheren Varianten geht die aktuelle Version das Thema Anwendungsmigration praxisorientiert und nicht ideologisch an und behandelt daher auch die Ablösung von Open-Source-Software.




## Barrierefreie Dokumente beim BSI

Mit der Migration seiner rund 500 PC-Arbeitsplätze auf Staroffice steht das Bundesamt für Sicherheit in der Informationstechnik (BSI, www.bsi.bund.de) kurz vor dem Abschluss. Rund 90 Prozent der Anwender arbeiten inzwischen mit dem kommerziellen Pendant von Openoffice – etwa zu je gleichen Teilen unter Windows XP und Linux (Debian). Die Bonner Behörde hatte sich im Rahmen ihrer Open-Source-Strategie für einen Umstieg auf ODF als internes, plattformübergreifendes Dokumentenformat entschieden. Die externe Kommunikation erfolgt über PDF-Dokumente. Daher standen nur Openoffice sowie Suns kommerzielles Pendant Staroffice zur Wahl. Letzteres erhielt in der Version 8 wegen der Support-Optionen den Zuschlag.

Für die Umstellung der hausinternen Dokumentenvorlagen zog man mit der Leverkusener SCAI GmbH (www.scaimas.de) einen externen Migrationsspezialisten hinzu. Durch die enge Zusammenarbeit im Rahmen des Projekts überarbeitete man den PDF-Exportfilter so, dass die BSI-Mitarbeiter jetzt einfach via „Exportieren als PDF“ barrierefreie PDF-Dokumente erstellen und so dem seit 2002 bestehenden Rechtsanspruch blinder und sehbehinderter Menschen auf barrierefreie Kommunikation mit Behörden gerecht werden können. Die Änderungen flossen in die Openoffice-Entwicklung zurück und sind im jetzt freigegebenen Update auf Version 2.4.1 schon enthalten.

iX-Link ix0807010

JavaOne 2008

# Nichts Neues im Westen

**Arno Puder, Lars Röwekamp**

Motto der dreizehnten JavaOne-Konferenz war „Java + You". Das Personalpronomen sollte erstmals auch für den Anwender, nicht nur für den Entwickler stehen.

Hätte man nicht bereits im letzten Jahr eine nahezu identische Präsentation während der JavaOne-Keynote gesehen, wäre die Ankündigung von JavaFX diesmal sicher auf mehr Begeisterung gestoßen. Zur Erinnerung: Mit JavaFX möchte Sun den Markt für RIA (Rich Internet Applications) revolutionieren und die Konkurrenten Microsoft (Silverlight) und Adobe (Flash/Flex und Air) das Fürchten lehren. Diese Angst sollen Anwendungen auslösen, die sowohl in einem Browser Plug-in als auch auf dem Desktop laufen. Der Clou dabei: Anwender ziehen sie aus dem Browser auf den Desktop und speichern sie dort – schon sind sie auch ohne Webbrowser nutzbar.

Merkwürdig mutete es vor allem an, dass Sun in der Keynote kein Wort zu dem Déjà-vu-Effekt verloren hat. Lediglich auf Flurgesprächen war zu hören, dass der letztjährige Entwurf der JavaFX Scripting Language und Runtime Engine eine komplette Überarbeitung benötigt hatte. Dies sei auch der Grund dafür, dass man zur diesjährigen JavaOne lediglich Demos vorweisen, den interessierten Entwicklern aber nichts Konkretes an die Hand geben konnte.

## Glassfish ist kleiner und schneller

Im Juli 2008 soll ein Early-Access-Programm des Desktop SDK starten, für das sich Entwickler bereits registrieren können. Version 1.0 des JavaFX Desktop will Sun im Herbst fertig haben. Bis zur mobilen Variante der Runtime Engine und JavaFX TV 1.0 dauert es jedoch noch bis Frühjahr nächsten Jahres.

Still und leider viel zu heimlich verbessert sich der freie Java-EE-Server Glassfish von Release zu Release. Mittlerweile kommt er in der Version 3 dank stark modularisierten Aufbaus mit einem Kernel von lediglich 98 KByte und einer Startzeit von nur einer Sekunde aus, was neue Perspektiven und Einsatzgebiete eröffnet. Neben klassischen Eigenschaften eines Application-Server wie Verfügbarkeit und Skalierbarkeit zeichnet sich der neue Glassfish vor allem durch die direkte Unterstützung von Java EE 6, OSGi und dynamischen Skriptsprachen wie JRuby aus.

Als Hydrazone bezeichnet man die von Hydrazin und seinen Derivaten gebildeten Iminanalogen Stoffe, die durch die Kondensation mit Carbonylverbindungen entstehen (Quelle: Wikipedia). Sun dürfte bei der Wahl des Namens für seine „Hydrazone"-Plattform vermutlich weniger an diese Definition als an den Einsatz der Chemikalien für den Raketenantrieb gedacht haben. So zumindest ist die Aussage zu verstehen, dass Services die Raketen der Zukunft seien, die alles antreiben werden.

Hydrazone soll als Open-Source-, Open-Standard-Service-Plattform dienen und Anbietern von Diensten eine Möglichkeit offerieren, sogenannte Cloud Services potenziellen Benutzern – bei Bedarf gegen Bezahlung – zur Verfügung zu stellen. Starten soll das Projekt mit einigen vorgegebenen, allgemeinen Services unterschiedlicher Granularität. Dazu gehören Kalenderfunktionen, Identity Management und Disk- beziehungsweise Datenbank-Dienste.

Wie immer nutzte Sun die Veranstaltung auch dafür, die allgemeine Java-Entwicklung aufzuzeigen. In seinem Vortrag ging Neal Gafter, Angestellter von Google und Editor der Java Language Specification, auf zukünftige Trends und Erweiterungen der Programmiersprache ein. Insbesondere erläuterte er die in Java 7 neu zu erwartenden Erweiterungen.

Dazu gehört unter anderem Multi-Catch: Eine *catch*-Klausel kann mehrere Exceptions unterschiedlichen Typs fangen. Annotationen sind in Zukunft nicht nur bei Deklarationen, sondern überall dort einsetzbar, wo Typen erlaubt sind. Das erlaubt Konstrukte wie *List <@NotNull String>* (Liste von Strings, die nicht Null sein dürfen). Weiterhin wird Java 7 ein lang vermisstes Modulkonzept einführen: Das Schlüsselwort *module* fasst Java Packages zu einem Modul zusammen und definiert die Sichtbarkeit der in ihnen enthaltenen Klassen. Andere Erweiterungswünsche werden laut Gafter wohl nicht umgesetzt. Dazu gehören Makros und das Überladen von Operatoren.

## Nicht mehr nur Java in der VM

Ein zentrales Thema der diesjährigen JavaOne war die Unterstützung von Skriptsprachen in der Java VM. Lange Zeit wollte Sun nur Java als Programmiersprache auf der VM zulassen. Microsofts .Net hingegen kann mit seiner VM verschiedene Sprachen verarbeiten. Vielleicht wegen des Drucks aus dem Microsoft-Lager ändert Sun nun seine Einstellung zu diesem Thema. Allerdings will es sich auf die Unterstützung von Skriptsprachen konzentrieren. Da sie jedoch oft dynamische Konstrukte benutzen, die das Abbilden auf eine VM erschweren, ist Sun sogar bereit, seine virtuelle Maschine mit Erweiterungen auszurüsten. Diese Aktivitäten sind im Da-Vinci-Projekt zusammengefasst, das die VM für andere Programmiersprachen außer Java attraktiv machen soll. Hierzu gehört insbesondere die Dynamic Invocation.

Interessant ist übrigens, dass auch die Erfinder der verschiedenen Skriptsprachen erkannt haben, wie schwer es ist, eine performante und sichere Runtime Engine zu schreiben. In einer Podiumsdiskussion waren sich nahezu alle einig darüber, dass die Verwendung der Java VM ihre Skriptsprache deutlich beschleunigen wird.

Eine weitere Podiumsdiskussion beschäftigte sich mit der Frage, inwieweit eine Welt von Open-Source-Projekten überhaupt noch offene Standards benötigt. Die Frage zielte vor allem auf den als träge bekannten und zum Teil sehr theoretisch aufgesetzten Java Community Process. Das wohl treffendste Statement hierzu gab Rod Johnson ab, Erfinder des Spring Framework und selbst Expert-Group-Mitglied mehrerer JSRs. Er meint, man solle lediglich wohlverstandene und in der Praxis erprobte Verfahren auf einem relativ niedrigen Level standardisieren – dies dann aber zwingend. Als positive Beispiele der Vergangenheit nannte er Socket Connections und JDBC. Schwieriger sei es dagegen bei Frameworks oder am Reißbrett entstandenen Techniken.

Wie immer war die JavaOne – alleine wegen der schieren Menge von Entwicklern aus aller Welt – ein besonderes Ereignis. Positiv zu bewerten ist Suns stärkere Öffnung für neue Welten und Trends. Beispielsweise wird es für verschiedene etablierte Entwurfswerkzeuge Plug-ins für den JavaFX-Export geben. Damit berücksichtigt Sun zum ersten Mal auch eine Zielgruppe außerhalb der klassischen Java-Entwicklergemeinde. Ein weiteres Beispiel ist die zukünftige Unterstützung dynamischer Skriptsprachen in der Java VM. Andererseits irritiert es, dass Sun zum zweiten Mal in Folge dieselbe Technik ankündigt, ohne Konkretes vorweisen zu können. Hoffentlich ist dies tatsächlich einem kompletten Redesign und einer damit verbundenen echten Verbesserung geschuldet. Eine dritte Chance wird Sun sicherlich nicht bekommen. (ck)




Europäische Veranstaltung für Webapplikations-Sicherheit

# Sicherheit 5.0

**Dirk Wetter**

**Im Entwurf des neuen HTML-5-Standards sind einige dringliche Sicherheitsvorgaben umgesetzt – eine Garantie für mehr Websicherheit ist das aber noch lange nicht, war bei der Konferenz des Open Web Application Security Project zu erfahren.**

Im Mai führte das Open Web Application Security Project (OWASP) seine 2004 ins Leben gerufene Hauskonferenz zur Webanwendungs-Sicherheit „AppSec“ durch. Sie findet halbjährlich, in Europa im Jahresturnus statt.

Mit Zitaten wie Bruce Schneiers „If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology“ traf OWASP-Mitbegründer Mark Curphey – vormals Foundstone, nun Microsoft – in der ersten Keynote zwar den Nagel in puncto Websicherheit auf den Kopf. Mehr inhaltlichen Tiefgang hatte er aber nicht zu bieten.

Anders Gary McGraw von Cigital. Sein Beitrag „Exploiting Online Games“ war zwar nicht 100 % kongruent mit dem Konferenzthema, allerdings baute er eine Brücke: Wie bei Javascript sind die Sicherheitsmaßnahmen beispielsweise bei „World of Warcraft“ (WoW) im Client verankert. Wer also im RAM die richtige Stelle findet, kann seine Figur schon mal aus kritischen Situationen herausteleportieren, eine Harley „herbeipoken“ oder „Items“ duplizieren. Eine serverseitige Überprüfung findet dabei nicht statt.

„The Warden“ – ein Spyware-Prozess von WoW – versucht auf dem Client das Mogeln dadurch zu unterbinden, dass er die Desktop-Fenstertitel zum WoW-Server sendet. Da dies ein Userland-Prozess ist, schuf McGraw „The Governor“, der mit Adminrechten dem Wächterprozess das unterschiebt, was er erwartet. Strafbar seien derlei Manipulationen meist nicht, weil es ja den eigenen Computer betreffe. Man verletzte nur die EULA. Bedenklich ist allerdings, dass virtuelles und reales Geld einen Wechselkurs haben und solche Spiele mittlerweile der Geldwäsche dienen.

## Dilbert-Reinkarnation

In der zweiten Keynote „Software Security State of the Practice 2008“ beklagte McGraw, dass Code-Sicherheit noch nicht die Bedeutung habe, die sie verdiene. Gartner sähe zwar Zuwächse dort, wo man damit Geld verdient. Bei Firmen sei das Bewusstsein auf sämtlichen Ebenen aber wenig ausgeprägt. So kritisierte er die Fehlkommunikation zwischen Managern und Technikern, und ebenso mussten Manager und Anbieter einstecken, die noch nicht den Unsinn von reinen Blackbox-Tests bei Software und Sicherheitsanalysen verstanden hätten.

Der Hype SaaS bekam einen Dämpfer von John Heasman („Software as a Service, Security on the Sidelines“), da „Office 2.0“ verglichen mit seinem lokalen Pendant zusätzliche Gefahren mitbringe wie XSS, Session-Hijacking und Cross-Site Request Forgery (CSRF). Penetrationstests von Software-ISPs, die eigene Anwendungen hosten, seien in den meisten Ländern zudem strafbar. Er betonte überdies die prinzipiell geringe Vertraulichkeit der Office-Daten bei SaaS-Anbietern wie Google, Yahoo, Adobe oder Zoho.

Viele kleinere, interessante Open-Source-Projekte fanden ihren Weg auf die AppSec-Konferenz, darunter das Antisamy-Projekt (Samy hieß der XSS-Virus, der Myspace lahmlegte). Statt Blacklists, die zur Bekämpfung von XSS nie 100%ig funktionieren, verwendet AntiSamy für .Net und PHP eine API, die in Policy-Dateien vorhandene HTML-Whitelists verarbeitet. Orizon ist ein junges, vielversprechendes OWASP-Framework zur Sourcecode-Analyse (SCA). Leider unterstützt der Code-Parser derzeit nur Java.

## HTML reloaded

Laut dem Sicherheitsleiter des W3C Thomas Roessler scheint der Entwurf für den HTML-5-Standard (unterstützt von Firefox 3, IE 8, Opera 9.5, Safari 3.1) nicht ganz unkritisch zu sein. Obwohl nun endlich die „Same Origin Policy“ im HTML-Standard verankert wird – derzufolge der Browser nur Dokumenten oder Skripten aus einer Quelle und nicht von beliebigen Webseiten trauen soll – bleiben Sicherheitsdefizite.

So soll in HTML 5 das Ursprungsfenster von IFrames oder Javascript-Popups das jeweilige Folgefenster durch Javascript manipulieren können, egal von welcher Domain Letzteres kommt. Schlimmer: Bei neuen *postMessage()* können sich Browserfenster domainübergreifend Zeichenketten per Javascript schicken, was einen ganzen Sack von Bedrohungen mit sich bringt – etwa Cross-Site Scripting und korrektes Parsing auf der Empfängerseite.

Die nächste „OWASP AppSec“ findet im Mai 2009 in Krakau statt. (ur)



XTech: Soziale Netze und mobiles Web

# Web-Dubliners

**Henning Behme**




Ajaxifiziert, mit Mikroformaten und ein bisschen RDF plus Sicherheit – so könnte ein Teil der sozialen Netze demnächst „gestrickt“ sein.

Unter dem Motto „The Web on the Move“ versammelte die diesjährige XTech Conference in Dublin vor allem Beiträge zu sozialen Netzen und Ajax. Außerdem ging es um die weitere Entwicklung im Browserbereich sowie die Portabilität von Daten.

So resümmierte Michael Smith (W3C) die jüngste Entwicklung auf dem Browsermarkt, wo das iPhone mit Safari den ersten „richtigen“ mobilen Browser enthält. Mit Opera mini, das die Engine von Opera 8.5 beinhaltet und schon auf Googles Android portiert ist, gibt es Konkurrenz. Außerdem, so Smith, werde es neue auf Webkit aufsetzende Browser für Windows Mobile geben.

Ob Mikroformate wie hCard oder XFN, ob entstehende Standards wie OAuth oder die kürzlich vorgestellte Google-API OpenSocial (siehe S. 90), immer wieder drehte es sich darum, wie soziale Netze sicher und komfortabel programmierbar sein können.

Wie man Ajax-Anwendungen schneller macht, war ebenso Thema wie fortgeschrittenes CSS-Layout und clientseitige Cross-Site-Anfragen. Und Richard Cyganiak vom irischen DERI führte unter anderem vor, wie weitverbreitet das als zu kompliziert geltende RDF sei: Außer Google und Yahoo nutzen es sowohl Reuters als auch die BBC.

## Rufverwaltung in der eigenen Hand

Mary Ann Malloy (Mitre) warb dafür, sich um den eigenen Onlineruf (Online Reputation Management) zu kümmern. Dazu wies sie darauf hin, dass bei einer Umfrage 60 % der US-Firmen angegeben hätten, Online-Checks bei möglichen Angestellten durchzuführen. 43 % hätten deswegen schon Kandidaten abgelehnt.

XML-Standards und ihre weitere Entwicklung sind traditionell Thema dieser Konferenz. So referierte Michael Kay über neue Eigenschaften in XML Schema 1.1: Conditional Type-Assignments (CTA) und Assertions. Dave Orchard sprach ergänzend über Versionierung von XML mit XML Schema. Außerdem war die Entwicklung von XQuery Inhalt mehrerer Vorträge

Unter „Presentations“ sind auf der Konferenz-Site (siehe *iX*-Links) einige Vorträge als PDF zu finden, meist allerdings nur die Slides. Dennoch nachlesenswert: Simon Wardleys Hauptvortrag „Why ‚Open‘ Matters – from Innovation to Commoditisation“, in dem er beschrieb, wie neue Ideen sich im Laufe der Zeit in Gebrauchsgegenstände verwandeln. Offene Standards, so Wardley, seien dafür von zentraler Bedeutung.

Das Zehnjährige der Auszeichnungssprache XML durfte nicht fehlen. Liam Quin vom W3C führte vor, wie omnipräsent die Sprache mittlerweile ist, indem er Anwendungsbeispiele aus aller Welt referierte. Sein Blick in die Zukunft richtete sich vor allem darauf, dass XML mit der Entwicklung von Unicode Schritt halten müsse, ohne die Kompatibilität zu XML 1.0 aufzugeben. Momentan hinke XML da hinterher.

Vorschläge für XML 2.0 gebe es zwar, die Umsetzung dürfte allerdings mindestens fünf Jahre dauern. Wahrscheinlicher sei die Zusammenführung bislang getrennter Spezifikationen wie Namensräume, Signaturen et cetera. (hb)

*iX*-Link ix0807015

Neue Scoring-Regelungen unter Beschuss

# Zweischneidig

**Ute Roos**

Jahrelang wetterten die Datenschutzbeauftragten gegen Handhabung und mangelnde Transparenz des Scorings in der Kreditwirtschaft. Nun legt der Gesetzgeber verbraucherfreundlichere Regelungen vor – und stößt überraschend auf Widerstand seitens der Datenschützer.

Nach den staatlichen Überwachungsthemen der vergangenen Jahre widmete sich die diesjährige Euroforums-Datenschutzkonferenz verstärkt der Privatwirtschaft. „Datenschutz ist up to date“, verkündete der Bundesdatenschutzbeauftragte Peter Schaar in seiner Eröffnungsrede, wenngleich die Anlässe für die zunehmende Publizität nicht immer positiv seien.

So sorgten die korrigierenden Urteile des Bundesverfassungsgerichtes zu nicht verfassungsgemäßen Gesetzen oder Überwachungsskandale à la Lidl bei vielen für eine zunehmende Sensibilisierung. Auf der anderen Seite stellen immer mehr Menschen immer mehr Informationen über sich ins Internet. Die Süddeutsche prägte für diesen elektronischen Exhibitionismus den Begriff „Orwellness“.

Das Innenministerium arbeite derzeit an einem Datenschutzauditgesetz, ein erster Entwurf liege vor, berichtete Schaar von neuen Gesetzesinitiativen. Ebenfalls neu ist die sogenannte „kleine Datenschutznovelle“, die kurz vor der Konferenz im Entwurf veröffentlicht wurde. Sie befasst sich vor allem mit neuen Regelungen für Auskunfteien, die Daten an die Wirtschaft weiterleiten. Der Gesetzgeber will den Daten- und Verbraucherschutz stärken und verpflichtet die Auskunfteien zu mehr Transparenz.

Sie müssen laut zukünftigem Bundesdatenschutzgesetz offenlegen, welche Faktoren sie zur Bewertung der Zahlungsfähigkeit eines potenziellen Kunden heranziehen, außerdem besteht dann für die Scoringbildung eine Dokumentationspflicht. Betroffene sollen einmal jährlich kostenlos Auskunft über sich erhalten. Wenngleich noch nicht geregelt ist, welche Daten an Dritte weitergegeben werden, begrüßt Schaar die Gesetzesnovelle ausdrücklich.

## Lähmt BDSG-Novelle die Wirtschaft?

Nicht so einige Datenschutzkollegen. „BDSG-Novelle ante portas – Ende von Auskunftsdiensten und Scoring?“ lautete der provokante Titel des Vortrags von Ralf Abel von der Fachhochschule Schmalkalden. Seiner Einschätzung nach hat der Gesetzgeber mit dem Entwurf eine bürokratische und unverhältnismäßige Regelung vorgelegt, die dem Verbraucher keinen echten Vorteil verschafft, der Wirtschaft aber Steine in den Weg legt und ihre Geschäftstätigkeit erschwert.

Als Beispiele nannte er unter anderem den Wegfall von Geschäftsgeheimnissen durch die neuen Transparenzregeln. Auch monierte er die späte Herausgabe von Daten über offene Forderungen. Für das betroffene Unternehmen klaffe damit eine viel zu lange Informationslücke zwischen der Fälligkeit einer Forderung und der Auskunft über den Schuldner, die erst acht Wochen nach der ersten Mahnung erfolgen darf. Summa summarum sieht er keinen Sinn in einer Novelle, die niemandem Vorteile bringt.

Welche Änderungen stehen noch ins Haus? Das schon erwähnte im Entwurf veröffentlichte Datenschutzauditgesetz, das allerdings nur die konkrete Durchführung eines solchen Audits regelt, jedoch niemanden dazu verpflichtet. Nach Ansicht der Datenschützer kann es Unternehmen aber einen Marktvorteil verschaffen, wenn sie sich durch nachweislich datenschutzkonforme Praktiken von ihrer Konkurrenz abheben.

Weiter beschäftigt sich der Gesetzgeber derzeit mit dem vom Bundestag beschlossenen Arbeitnehmerdatenschutzgesetz, allerdings, wie zu hören war, ohne große Eile. Einigen Anwesenden stellte sich ohnehin die Frage nach dessen Notwendigkeit, da die grundlegenden Sachverhalte durch gesetzliche Grundlagen im Personalaktenrecht, Betriebsverfassungsgesetz oder Bundesdatenschutzgesetz abgedeckt sind. Überwachungsskandale wie jüngst bei einigen Lebensmitteldiscountern halten die Diskussion über ein neues Gesetz aber in Gang.

Auf europäischer Ebene können Unternehmen in Kürze mit dem sogenannten EuroSOX rechnen, Experten erwarten die Veröffentlichung im Bundesgesetzblatt Mitte des Jahres. Der europäische Bruder des amerikanischen Sarbanes-Oxley Act (SOX), der Regelungen zu Haftung, Transparenz et cetera in börsennotierten Unternehmen enthält, soll strenger sein als das Original.

Optimistisch zeigte sich der Europäische Datenschutzbeauftragte Peter Hustnix. Zwar sei es im Zeitalter der Globalisierung im Rahmen internationaler Transaktionen schwierig, datenschutzkonform zu bleiben, und ein weltweiter Standard wäre gut. Im Vertrag von Lissabon, der am 1. Januar 2009 in Kraft treten soll, sieht er aber mit Artikel 7 und 8 der EU-Charta (Achtung des Privat- und Familienlebens und Schutz personenbezogener Daten) sowie Artikel 6 des EU-Vertrags (Achtung der Grundrechte) die Voraussetzung für einen effektiven, auch internationalen Datenschutz gegeben – was nicht nur angesichts der europäischen Zusammenarbeit von Polizei und Justiz erforderlich ist.




**Der Entertainer: Thomas Hoeren von der Universität Münster ist bekannt für seine unterhaltsame Darlegung spektakulärer und absurder Gerichtsurteile aus der IT-Welt.**

## Schlimmer, bevor es besser wird

Etwas weniger optimistisch schaut Andy Müller-Maguhn vom Chaos Computer Club in die Zukunft: Die Verwertung der massenhaft gesammelten Daten von Wirtschaft und Behörden im Antiterrorkampf habe angefangen. Zwar würde die Diskussion auch wieder in die andere Richtung gehen und das Bundesverfassungsgericht reduziere mit seinen Urteilen staatliche Datengelüste, aber vorher komme erst einmal die Phase der Katastrophen und der Daten-GAUs. (ur)

## OpenVAS tritt die Nachfolge des Netz-Scanners Nessus an

Der bekannte Netz-Scanner Nessus (www.nessus.org) ist seit einiger Zeit nicht mehr als freie Software erhältlich, da neue Versionen ausschließlich unter einer proprietären Lizenz erscheinen. Dies betrifft auch die als „Plugins“ bezeichneten einzelnen Tests auf Sicherheitslücken.

Das Projekt OpenVAS schließt jetzt diese Lücke (www.openvas.org). Es baut auf den letzten frei verfügbaren Quellen von Nessus auf und entwickelt sie weiter. Mittlerweile sind funktionierende und stabile Versionen sowohl der Server- als auch der Client-Komponente verfügbar, Letztere auch für Windows. Damit lassen sich von jetzt an die nun NVT (Network Vulnerability Test) genannten „plugins“ entwickeln. Die Entwicklung von OpenVAS treibt in Deutschland vor allem das Bundesamt für Sicherheit in der Informationstechnik (www.bsi.bund.de) voran, aber auch die internationale Community ist zunehmend aktiv. OpenVAS steht als freie Software unter der GPL zur Verfügung.

Der OpenVAS-Scanserver kommt an zentraler Stelle für Sicherheitsprüfungen von Systemen im Netz zum Einsatz. Der OpenVAS-Client steuert die Prüfungen, kann lokale Prüfmodule mit dem Security Local Auditing Daemon (SLAD) durchführen und speichert die Prüfergebnisse für die Auswertung. Die Software-Suite enthält unter anderem ein Werkzeug zum automatisierten Nachladen einer kontinuierlich wachsenden Zahl an NVTs von der OpenVAS-Website.

*Christian Böttger*

## BMBF fördert „Digitales Produktgedächtnis“

Mit der Innovationsallianz „Digitales Produktgedächtnis“ wollen Wirtschaft und Wissenschaft die notwendigen Bausteine für das „Internet der Dinge“ in der Logistik erforschen und entwickeln. Während RFID-Systeme die eindeutige Identifizierung von Produkten erlauben, geht die Allianz und das zugehörige Projekt namens SemProM (Semantic Product Memory, www.semprom.de) einen Schritt weiter: Eingebettete Computersysteme werden sich im Produkt oder in der Verpackung befinden, so die Vorstellung der Allianz, die das Bundesministerium für Bildung und Forschung initiiert hat. Sie enthalten einen Mikroprozessor, Speicher, Mikrosensor-Systeme, GPS-Chip, Funkbausteine und eine eigene Energieversorgung.

Sensoren sammeln Daten über Temperatur, Helligkeit, Feuchtigkeit, Geschwindigkeit, Lage oder Beschleunigung und speichern die Werte lokal am Produkt. Darüber hinaus merken sich die eingebetteten Systeme alle produktrelevanten Daten und können mit anderen Gegenständen und Nutzern in ihrer Umgebung aktiv Informationen austauschen.

Zentrale Rechner zur Steuerung des Warenflusses sollen damit entfallen. Diese Aufgabe übernehmen die Produkte selber – sie kennen ihr Ziel und ermitteln den besten Weg dynamisch. Hersteller, Lieferanten, Händler und Verbraucher sollen nach den Vorstellungen der Projektbeteiligten die Produktinformationen jederzeit abrufen können.

*Barbara Lange*

## KURZ NOTIERT

**Malware-Schutz:** Ebertlang, Gießen, vertreibt den Spam- und Malware-Schutz von Alt-N Technologies in Deutschland, Österreich und der Schweiz. Das „Security Gateway für Exchange/SMTP“ des texanischen MDaemon-Herstellers soll schädliche und unerwünschte E-Mails aus dem eigenen System fernhalten und arbeitet sowohl auf Exchange- als auch auf anderen SMTP-Mailservern (www.ebertlang.com).

**Klare Prozesse:** Zusammen mit der Nürnberger Firma Knowledge Department hat die Berliner Microtool eine Variante ihrer Projektmanagementsoftware in-Step entwickelt: die Spice Edition for Automotive. Sie hilft beim Planen und Durchführen von Projekten auf Spice Level 3 und bietet Anforderungs-, Änderungs-, Risiko- und Ressourcenmanagement. Für alle geforderten Dokumente stehen Vorlagen zur Verfügung. Die Ergebnisse werden zentral versioniert. Eine Kennenlern-Edition gibt es kostenlos unter www.microtool.de/instep/de/download.asp.

**Krypto-Service:** Antispameurope aus Hannover bietet seinen Kunden neuerdings digitale E-Mail-Signaturen per S/MIME. Darüber hinaus lassen sich die E-Mails nun auf dem Transportweg mit TLS gegen Mitlesen durch Dritte schützen (www.antispameurope.de).

## EMC World: Flash-Laufwerke und Spin-Down

Auf seiner Hausmesse in Las Vegas stellte EMC zahlreiche Neuheiten vor. In seinem Flaggschiff Symmetrix etwa will der Hersteller spätestens ab Juni 2008 auch SSDs einsetzen. Existierende DMX-4 lassen sich nachrüsten, ältere Symmetrix-Systeme hingegen nicht.

Laut EMC sind die Flash-Speicher beim Schreiben vier- bis sechsmal schneller als FC-Festplatten (73 GByte, 15 000 U/min), beim Lesen sogar bis zu dreißigmal. Auf welches Maß sich die Angabe bezieht, hat der Hersteller vergessen zu erwähnen. Allerdings kostet eine SSD momentan etwa 20-mal so viel wie ein FC-Laufwerk. EMC rechnet jedoch mit einem drastischen Preisverfall und will bis 2010 alle FC-Platten durch SSDs ersetzen.

Mit den Disk-Libraries DL 3D 1500, 3000 und 4000 ergänzt der Hersteller sein Angebot an Backup-Systemen. Die Modelle 1500 und 3000 enthalten in der Grundausstattung vier beziehungsweise acht SATA-Festplatten – zum Einsatz sollen ausschließlich die 1-TByte-Modelle von Western Digital kommen – und lassen sich auf 36 respektive 148 Platten ausbauen. Beim kleinen Modell stehen sechs GE- und zwei 4-GBit-FC-Anschlüsse zur Verfügung, bei der DL 3D 3000 jeweils zwei mehr. Im Gegensatz zu früheren Modellen beherrschen die integrierten RAID-Controller nun auch den RAID-Level 6 (Double Parity).

Für die nicht vor der Jahresmitte verfügbare 4000er-Serie sieht EMC eine Stromspartechnik namens „Spin-Down“ vor. Sie versetzt ungenutzte Festplatten in den Ruhezustand und soll dadurch den Energiebedarf um 47 % reduzieren. Preise und weitere Details nannte der Hersteller nicht.

Alle Disk-Librarys arbeiten mit Quantums Deduplizierungstechnik. Sie spürt vor dem Schreibvorgang in Datenblöcken variabler Größe (1 bis 32 KByte) sich wiederholende Muster auf und ersetzt sie durch Verweise. Die sogenannte In-Band-Technik hat allerdings den Nachteil, dass die VTL die Daten nur so schnell entgegennehmen kann, wie die Deduplizierungs-Engine sie verarbeitet.

Sozusagen an der Quelle dedupliziert die neue Version der Backup-Lösung Avamar. Ein Agent auf dem zu sichernden System entfernt Wiederholungen und reduziert dadurch den Datenstrom zum Storage-System. Allerdings steigt dadurch die CPU-Last auf dem Backup-Client. *Ulrike Rieß*

### KURZ NOTIERT

**Alles offen:** Die Teilnehmer des Open Graphic Projects sind nun in der Lage, die erste Open-Source-Grafikkarte OGD1 zu produzieren und nehmen Bestellungen entgegen. Noch ist das Board nur für Entwickler gedacht und soll 1500 US-Dollar kosten.

**Innen kühl:** IBM hat die von seinem Züricher Forschungslabor 2006 vorgestellte „High Thermal Conductivity Interface Technology“ in Zusammenarbeit mit dem Fraunhofer Institut für Zuverlässigkeit und Mikrointegration (IZM) in erste Prototypen umgesetzt. Diese Wasserkühlmethode für gestapelte Chips pumpt Wasser durch etwa 50 Mikrometer feine Strukturen direkt zwischen die einzelnen Prozessorebenen, das den ganzen Chip von innen kühlt.

**Doppelt modular:** Hewlett-Packard hat mit dem Storageworks 9100 Extreme Data Storage System (HP ExDS9100) ein modulares NAS-System vorgestellt. Durch die Unterteilung in mehrere NAS-Köpfe und Speichermodule lassen sich Speicherkapazität und Durchsatz unabhängig voneinander skalieren. Als NAS-Server-Köpfe benutzt HP seine Blade-Systeme, bestehend aus 4 bis 16 Blades mit Gigabit Ethernet.
Der Speicherblock besteht aus drei bis zehn Festplatten-Chassis mit je 82 TByte. Im vierten Quartal soll das System verfügbar sein.

## HDDS und SSDs: Alten- und Kinderpflege

Viele halten Magnetplatten für veraltet, doch die Hersteller entlocken ihnen immer neue Verbesserungen. Toshiba etwa sieht für seine beiden neuen 1,8"-Platten mit 80 (MK8017 GSG) und 160 GByte Kapazität (MK1617GSG) aufgrund des weiter wachsenden Markts für Highend-Notebooks eine rosige Zukunft. In den Laufwerken rotieren ein beziehungsweise zwei Magnetscheiben (Platter) mit 5400 RPM. Der Durchsatz der Schnittstelle nach SATA 2.6 liegt bei 1,5 GBit/s, die Leistungsaufnahme bei 0,5 Watt.

Hitachi und Fujitsu drehen ebenfalls an der Kapazität und der Umdrehungszahl, allerdings bei den 2,5"-Platten: Die Kapazität von 320 GByte bei 7200 RPM und einem 3 GBit/s schnellen SATA-II-Interface ist den Modellen Fujitsu MHZ2 BJ und Hitachi Travelstar 7K320 gemein. Unterschiede finden sich in der Leistungsaufnahme: Während sich Hitachis 7K320 mit 1,8 Watt im Schreib- und Lesebetrieb (0,8 Watt im Idle-Modus) begnügt, genehmigt sich Fujitsus MHZ2 BJ gern 2,3 Watt während der Arbeit. Die Notebook- und Desktop-Platten sollen bereits im Juni verfügbar sein. Warten muss dagegen die Server- und Storage-Fraktion auf die Versionen für den Dauerbetrieb. Das Modell MHZ2BK soll im Juli 2008 auf den Markt kommen, Hitachis Angaben zum Erscheinungstermin der 7K320-24-Stunden-Version sind mit dem dritten Quartal 2008 etwas vager gehalten.

Bereits Anfang des Jahres hatte Hitachi der Welt eine Travelstar 5K500 genannte und 500 GByte bei 5400 RPM fassende 2,5"-HDD angedroht. Für die Kapazitätserhöhung hatte der Hersteller ihr eine weitere Scheibe spendiert, dadurch verlangt sie bei einer Höhe von 12,5 mm ganze 3 mm mehr Platz, als viele Laptops bieten.

Im 3,5"-Segment schraubt Samsung an der Leistungsaufnahme. Die 1-TByte-Festplatte Ecogreen F1 soll im Betrieb zwischen 5 und 6,2 Watt, im Standby zwischen 0,5 und 0,8 Watt in Wärme umwandeln, also etwa halb so viel wie vergleichbare Modelle.

Derweil wollen die Hersteller von Solid State Disks (SSD) die Nachteile des designierten HDD-Nachfolgers beseitigen: den hohen Preis, die niedrige Geschwindigkeit und die geringe Kapazität. Samsung etwa arbeitet an einer 2,5"-SSD mit 256 GByte Fassungsvermögen, einer ansehnlichen Lesegeschwindigkeit von 200 MByte/s und einer Schreibperformance von 160 MByte/s. Außerdem verfügt sie über eine integrierte AES-Verschlüsselung. Während der Arbeit soll die Leistungsaufnahme konstant bei 0,9 Watt liegen – einer der Vorteile von SSDs. Bis Ende des Jahres will Samsung die Massenproduktion starten, eine 1,8"-Variante soll folgen.

An der Preisentwicklung arbeitet währenddessen IM Flash. Das Joint-Venture-Unternehmen von Intel und Micron hat die ersten NAND-Flash-Bausteine mit einer Strukturbreite von 34 Nanometern vorgestellt. In der zweiten Jahreshälfte soll die Serienfertigung der 172 $mm^2$ kleinen und 32 GBit fassenden Chips auf 300-mm-Wafern starten.

## 6- und 12-Kern-Opterons von AMD

Andere zu kritisieren schützt vor eigenen Fehlern nicht, nach diesem Motto hat sich AMD anscheinend entschieden, 2010 mit einer CPU aufzuwarten, die aus zwei Dice besteht. Während der Chip-Hersteller nicht müde wird, Intels Tigerton genannten Xeon 7300 dahingehend zu kritisieren, arbeitet er selbst bereits an einer 6-Kern-Opteron-Die, derer zwei den 12-Kern-Prozessor „Magny-Cours“ schmücken sollen. Der 6-kernige Single-Die-Opteron soll als „Istanbul“ noch 2009 das Licht der Welt erblicken. Zuvor steht aber mit „Shanghai“ (für zwei bis acht Sockel) und „Suzuka“ (für einen Sockel) noch der Umstieg auf den 45-nm-Prozess an. Glanzstück soll 2010 die Server-Plattform „Maranello“ mit dem Hypertransport-Switch „RD890S“ samt I/O-Virtualisierung und PCI-Express 2.0 werden.

## Supercomputer-Verbund Stufe 3

Anfang Mai 2008 ging bei der Max-Planck-Gesellschaft im Rechenzentrum Garching (RZG) bei München (MPG) ein neuer Superrechner in Betrieb. Der Power 575 von IBM im RZG soll im Endausbau mit 6600 Power6-CPUs im Cluster auf eine aggregierte Spitzenleistung von über 125 Teraflop/s kommen. Gemeinsam mit der vor Kurzem hochgerüsteten BlueGene/P im RZG entsteht der Rechnerverbund „HPMG 3 Komplex“, der den einst deutschlandweit schnellsten HPMG 2 Komplex ablöst. Damit kann das RZG sein Angebot an Rechenleistung für die Wissenschaft in Deutschland etwa um das Dreißigfache erhöhen. Der Energieverbrauch wächst dabei nur um den Faktor 3.



**Grüne Linie: Obwohl die Rechenleistung des Power 575 um das Dreißigfache wächst, braucht das System nur dreimal so viel Energie (Abb. 1).**

Pro 2U-Knoten baut IBM 16 Power6-CPUs mit je zwei Kernen ein, die wiederum über zwei Hardware-Threads verfügen. In einen Schrank passen 14 Knoten, jeder mit maximal 250 GByte Hauptspeicher. IBM verwendet die mit 4,7 GHz getakteten Power6-Prozessoren und kommt im SPEC CPU2006 mit 32 Kernen auf 934 SPECint_rate 2006 und 839 SPECfp_rate 2006 (www.rzg.mpg.de).

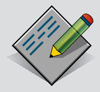
iX-Link ix0807020

## Einsteins These auf der Spur

Für einen ganz speziellen Zweck hat „Atlas“, der Cluster am Albert-Einstein-Institut (AEI) in Hannover, im Mai seinen Betrieb aufgenommen. Die Forscher der Max-Planck-Gesellschaft wollen damit die Gravitationswellen nachweisen, die Einstein vorhergesagt hat. Nun verfügt das AEI über weitere 5684 Prozessorkerne, 1,1 Petabyte Festplattenspeicher und eine kaskadierte 1- sowie 10-GBit-Ethernet-Vernetzung. In den Atlas-Knoten von Pyramid kommen 2,4 GHz schnelle Xeons von Intel mit je vier Kernen zum Einsatz. Bis zu 48 Nodes sind per 1-GBit-Ethernet über einen „Top-of-Rack“-Switch von Woven Systems verbunden, die wiederum über vier 10-GBit-Ethernet-Ports mit den anderen Cluster-Racks über einen zentralen 10-GE-Switch EFX 1000 kommunizieren, der auch die Verbindung zum SAN herstellt (www.pyramid.com).

iX-Link ix0807020



**Sonnenwende:** Mit Solaris 10 (x86) vorinstalliert liefert Fujitsu Siemens Computers (FSC) einige seiner „Industry Standard Server“ Primergy aus. Sun und FSC haben dazu ein OEM-Abkommen für mehrere Jahre unterzeichnet (www.sun.com).

**Freier Test:** SPECs Benchmark SPECjvm2008 für Java Virtual Machines ist unter dem SPEC Licence Agreement frei erhältlich. Er löst den betagten Vorgänger SPECjvm98 ab (www.spec.org/jvm2008).

**Sprachwende:** Eine Version in deutscher Sprache von Infrastructure 3.5 (VI3.5) hat VMware auf den Markt gebracht. Im Laufe des Jahres sollen weitere folgen: Virtual Desktop Management, Site Recovery Manager, ACE, VMware Player, Fusion und VMware Workstation (www.vmware.com).

iX-Link ix0807020

## SPEC überarbeitet CPU2006

Bei ihrer Prozessortestsuite CPU2006 hat die Open Systems Group (OSG) an mehreren Stellen Hand angelegt. Nur bei den eigentlichen Tests hat sich nichts verändert, die Ergebnisse der neuen Version V1.1 bleiben aber mit der früheren V1.0 vergleichbar. Neukunden bittet die SPEC mit 800 US-Dollar für die Suite zur Kasse, wer nur ein Upgrade von der CPU2000 braucht, zahlt die Hälfte, gemeinnützige Organisationen und von der SPEC anerkannte Bildungseinrichtungen bekommen die CPU2006 für 200 US-Dollar. Für Lizenznehmer der V1.0 gibt es die neue Version frei Haus.

Hauptanliegen der Entwickler war es, die bis dato schwere Handhabbarkeit des Softwarepakets zu erleichtern. Die CPU2006 soll nun einfacher und auf deutlich mehr Systemen installierbar sein. Bei Multi-Core-Systemen nutzen die Installationsroutinen parallele Mechanismen zur Beschleunigung. Dokumentierte Schnittstellen in den Testprogrammen zum Monitoring und die Option zum Abschalten der strengen Regelüberprüfung vereinfachen die Arbeit für Entwickler (www.spec.org/cpu2006).

iX-Link ix0807020

## Petaflops-Grenze durchbrochen?

Das US-Ministerium für Energie kündigt die Inbetriebnahme des „Roadrunner“ an. 2006 hatte IBM den Zuschlag für den neuen Supercomputer am Los Alamos National Laboratory (LANL) erhalten (*iX* 11/06, S. 34). Die Petaflop-Grenze soll das System am 25. Mai überschritten haben. Dazu lief der für die Top500 einschlägige Linpack-Test zwei Stunden ununterbrochen – allerdings nicht am LANL (www.lanl.gov).

Bei der Architektur handelt es sich um ein „Hybridsystem“: Rund 7000 Opteron- und 13 000 PowerXCell-8i-Prozessoren stellen insgesamt über 116 000 Recheneinheiten zur Verfügung. Die Opterons von AMD sollen ungefähr 50 Teraflop/s und die Cells von IBM 1,4 Petaflop/s leisten. Noch steht der Roadrunner in den IBM-Labors in Poughkeepsie. Dort sind drei Coding Teams des amerikanischen Energieministeriums mit ersten Tests beschäftigt. Der Aufbau und das endgültige Einrichten beim LANL sollen in den nächsten Wochen erfolgen.

Die Nationale Agentur für Nuklearsicherheit (NNSA) des Ministeriums nutzt den Superrechner zusammen mit den US-Streitkräften hauptsächlich zur Simulation von Nukleartests. Daneben kommen andere militärische Anwendungen zum Einsatz. Außerdem soll der Roadrunner die US-Truppen bei Auslandsmissionen unterstützen. Laut Dr. Michael R. Anastasio führt das Los Alamos Labor nach einer anfänglichen Periode des Tests und der Schulung innerhalb der ersten sechs Monate außerdem nichtmilitärische Projekte durch, etwa aus der Forschung über HIV oder Dunkle Materie. Später wäre eine Nutzung durch Universitäten und ausländische Körperschaften möglich. *Nikolai Zotow*

iX-Link ix0807020

## NEC baut neuen Earth Simulator

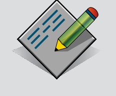
Vor allem zur Verbesserung der Vorhersage von Naturkatastrophen ist der neue Earth Simulator gedacht, für den NEC einen Auftrag erhalten hat. Der Supercomputer mit einer aggregierten Spitzenleistung von 131 Teraflop/s soll den bisherigen, ebenfalls von NEC stammenden Rechner am japanischen Forschungszentrum JAMSTEC (Japan Agency for Marine-Earth Science and Technology) ablösen. Im März 2009 will NEC den neuen Weltrechner in Betrieb nehmen (www.nec.com).



## Mail-Verschlüsselung „as a Service"

„Policy Based Encryption" nennt sich die neue Dienstleistung von Messagelabs. Sie ermöglicht Unternehmen und Behörden aller Größen, sämtlichen ein- und ausgehenden Mailverkehr nach festgelegten Regeln zu ver- und entschlüsseln. Durch Scannen nach bestimmten Begriffen oder Zahlenfolgen (etwa Kreditkartennummern), Überprüfen der Identität von Absendern und Empfängern et cetera soll der Versand vertraulicher Daten verhindert werden. Der Verschlüsselungsdienst ist laut Hersteller mit allen relevanten Plattformen einschließlich Blackberry und Windows mobile kompatibel. Er lässt sich überdies mit weiteren Diensten von Messagelabs wie Viren- und Spam-Abwehr und anderen kombinieren. Der vollständig beim Dienstleister verwaltete Service soll schnell einsatzbereit und für den Benutzer einfach zu bedienen sein.

## KURZ NOTIERT



**Virtualisierte Daten retten:** Der Datenrettungsspezialist Kroll Ontrack (www.krollontrack.de) bietet ab sofort die Wiederherstellung nicht mehr zugänglicher Daten auf VMware-Systemen an. Die Schwierigkeit dabei ist laut Kroll Ontrack das Ausfindigmachen der Fehlerquelle, die in einem Hardwaredefekt, aber auch in der Organisationsebene der Virtual Machine liegen kann.

**Botnetz-Analyse:** Wie Botnetze funktionieren, welche es gibt, welche Industrie dahintersteckt und wie sie sich historisch entwickelt haben, beschreibt Virenschutzhersteller Kaspersky in einem neuen Whitepaper. Das PDF „Botnetze – Geschäfte mit Zombies" können Interessierte kostenlos online herunterladen (*iX*-Link).

**RFID-Umfrage:** Bis Ende Juni können kleine und mittlere Unternehmen an einer Umfrage zum RFID-Einsatz teilnehmen (*iX*-Link). Hintergrund ist die Ermittlung der aktuellen Nutzung und zukünftiger Trends in Sachen RFID. Die Umfrage ist Teil des vom BMWi geförderten Projekts „RFID für kleine und mittlere Unternehmen".

**Spam-Firewall „für Große":** Für Internetprovider oder große Unternehmen mit bis zu 100 000 E-Mail-Benutzern und 5000 Domains hat Barracuda (www.barracudanetworks.com) seine neue Spam Firewall 1000 konzipiert. Sie ist für rund 85 000 Euro zu haben, benutzerabhängige Lizenzgebühren fallen nicht an.

**Geografischer IP-Filter:** Secure Computing (www.securecomputing.com) hat in seine Appliance-Reihe „Secure Firewall" eine Funktion zur geografischen IP-Filterung integriert. Auf die Art sollen Unternehmen Netzwerkprotokolle und Anwendungen aus Ländern blockieren können, mit denen sie keine Geschäftsverbindung unterhalten und die für Malware-Versand berüchtigt sind.

**Sicheres Drucken:** Eine Schwachstelle in Sachen Verlust vertraulicher Daten ist nach wie vor das Drucken. Das europäische BSI-Pendant ENISA hat für Unternehmen eine 22-seitige Empfehlung herausgegeben, wie man den Zugriff auf Druck-, Scan- und Kopierfunktionen sinnvoll reglementiert – durch Policy-beschränkung, Authentifizierung gegenüber dem Drucker, Klassifizierung der Dokumente et cetera. Das PDF ist kostenlos auf der ENISA-Website verfügbar (*iX*-Link).

**E-Commerce-Leitfaden:** Was man für den erfolgreichen Internethandel beachten sollte, fasst ein umfangreicher Ratgeber des Forschungsinstituts ibi reserch zusammen. Er vermittelt Wissenswertes rund um Geschäftsmodelle, Zahlverfahren, Risiken und vieles mehr. Den kostenlosen Leitfaden gibt es unter www.ecommerce-leitfaden.de.

*iX*-Link ix0807022

## Neue Modalitäten für Nessus-Plug-ins

Tenable Network Security (www.tenablesecurity.com), das Unternehmen des Nessus-Erfinders Renaud Deraison, das Weiterentwicklung und Aktualisierung des Schwachstellen-Scanners betreibt, wird nach gut vier Jahren am 31. Juli 2008 seine Politik für die Plug-in-Feeds mit neuen Updates ändern. Bisher gab es neben dem vergleichsweise leider dünnen GPL-Feed der Community ein „Registered" und ein „Direct Feed" von Tenable, wobei Letzterer in puncto Schwachstellenanalyse eine Woche voraus war und den Benutzer dafür 1200 US-Dollar pro Jahr kostete.

Beide Tenable-Feeds erscheinen künftig gleichzeitig. Der kostenfreie ist Privatanwendern vorbehalten, der dann auf den Namen „HomeFeed" hört. Hierfür ist eine neue Registrierung bis Ende Juli nötig. Bei der kommerziellen Variante bleibt außer dem neuen Namen „ProfessionalFeed" alles beim Alten. Gemeinnützige Organisationen und solche, die lehren, aus- oder fortbilden, dürfen den „ProfessionalFeed" umsonst nutzen.

*Dirk Wetter*




**Geändertes Geschäftsmodell: Kostenlose Aktualisierungen des beliebten Schwachstellen-Scanners Nessus gibt es nur noch für Privatanwender, Nutzer – ob privat oder aus Unternehmen – müssen sich in jedem Fall registrieren.**

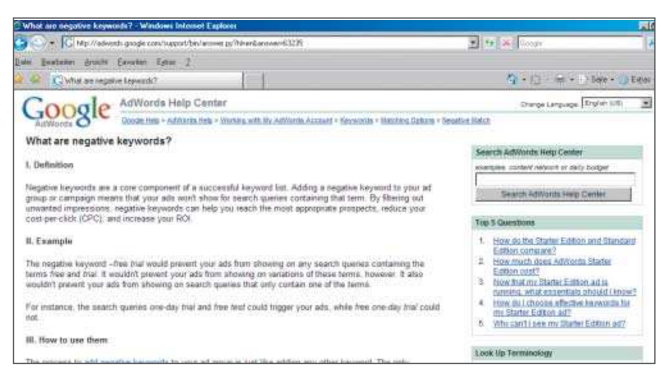
## Anruferauthentifizierung durch Sprache

Vergessene Passwörter und gesperrte Benutzerkonten gehören zu den häufigsten Gründen, einen Helpdesk anzurufen. Mit dem „Password Reset Management" will Siemens IT Solutions and Services die Abwicklung dieser Anrufe automatisieren. Das Produkt authentifiziert die Anrufer anhand ihrer Stimme und soll so die Administratoren entlasten. Vergessliche Nutzer sollen ihr Konto in wenigen Minuten automatisch durch die Stimme freischalten können, indem sie einer Computerstimme ein paar zufällig generierte Zahlenkombinationen vorlesen. Das biometrische Template erstellt das System automatisch bei der Registrierung. Hierfür muss der Nutzer den Text einer verschlüsselten E-Mail am Telefon vorlesen. Die Freigabe erfolgt automatisch, ohne Eingriff der Helpdesk-Mitarbeiter. Das Produkt integriert die Software „Voice Password Management" des Stuttgarter Unternehmens Excelsis Business Technology AG (www.excelsisnet.com/voice/de).

*Barbara Lange*

## USA: „Negative keywords“ Pflicht

Sollte das Urteil eines Gerichtes aus Florida auch hierzulande Schule machen, könnten Anbieter von Webseiten zukünftig verpflichtet sein, negative Schlüsselwörter zu verwenden, um eine Markenverletzung zu verhindern. Einem Unternehmen war die Verwendung einer bestimmten Marke verboten worden. Die US-amerikanischen Richter verurteilten es auch dazu, bei gängigen Suchmaschinen das Auffinden der eigenen Webseite bei Suche nach eben dieser Markenbezeichnung auszuschließen, damit die Webseiten des Rechtsverletzers bei einer Suche nach der geschützten Marke erst gar nicht als Suchergebnis ausgegeben werden. Bei Google ist dies unter der Einstellung „negative keywords“ möglich, bei Yahoo unter „excluded words“. Etwas bizarr mutet es schon an, wenn der Markenrechtsverletzer dazu verurteilt wird, die Marke – allerdings nur in diesen Einstellungen – zu nutzen. Aus technischer Sicht ist das aber sicherlich ein effizientes Mittel, Markenmissbrauch in Internet-Suchmaschinen zu vermeiden. *Tobias Haar*




**Mit sogenannten negativen Keywords lässt sich die missbräuchliche Eintragung von Marken in Internet-Suchmaschinen verhindern. Ein US-Gericht hat jetzt ein Unternehmen zu deren Nutzung verurteilt.**

## Gebäude können ein Namensrecht haben

Der Eigentümer des Grundstücks, auf dem das „Schloss Eggersberg“ steht, hat an dieser Bezeichnung ein Namensrecht, entschieden die Richter am Landgericht München I (Az. 33 O 15411/07). Sie verurteilten die Inhaberin einer .de-Domain, die diese Bezeichnung als Domainnamen gewählt hatte, zur Löschung. Hier liege eine Namensanmaßung vor, die zu einer Zuordnungsverwirrung führe, so die Richter. *Tobias Haar*

## Unerlaubte WLAN-Nutzung als Straftat

Nach Auffassung des Amtsgerichts Wuppertal (Az. 22 Ds 70 Js 6906/06) ist die unerlaubte Nutzung eines privaten offenen WLAN-Hotspots ein strafbares Abhören von Nachrichten und ein Verstoß gegen die Strafvorschriften im Bundesdatenschutzgesetz (s. S. 3). Andere Gerichte lehnten bislang eine strafrechtliche Ahndung solcher Handlungen ab. Den Geschädigten standen damit nur zivilrechtliche Schadensersatzansprüche gegen den Schwarznutzer zu. Der Täter im vorliegenden Fall wurde nur zu einer geringen Strafe verurteilt, da die Rechtslage „bislang ungeklärt war“, so die Richter. *T. Haar*

## Neues Schweizer Urheberrecht tritt in Kraft

Am 1. Juli 2008 treten die Änderungen des schweizerischen Urheberrechts in Kraft. Zu den wesentlichen Änderungen zählt, dass künftig nicht mehr nur Urheber über die Verwendung ihrer Werke und Leistungen im Internet bestimmen dürfen, sondern ebenso Interpreten, Produzenten und Sendeunternehmen. Einen besonderen Schutz erhalten auch Kopier- und Zugangssperren gegen unerlaubte Werkverwendung. Ungewöhnlich ist der Ansatz, eine „Beobachtungsstelle für technische Maßnahmen“ zu schaffen. Sie hat „Auswirkungen der Anwendung von Maßnahmen wie Zugangs- oder Kopiersperren auf die erlaubten Werkverwendungen zu beobachten, allfällige Probleme zu orten und durch Vermittlung zwischen den Betroffenen einvernehmliche Lösungen herbeizuführen“. *T. H.*

## KURZ NOTIERT

**Onlinearchive:** Archivcharakter muss sich nicht aus URLs ergeben. Es genügt, wenn dies aus den näheren Umständen ersichtlich ist. Das entschied das Kammergericht Berlin. Wichtig ist die Entscheidung, da Namensnennungen von Straftätern beispielsweise nach einer gewissen Zeit nur noch in Archiven, nicht mehr aber im aktuellen Webangebot gestattet sind.

**Anwalts-Linux:** In Version 2.0 steht die Anwaltssoftware Advolux des gleichnamigen Herstellers (www.advolux.de) erstmals auch für Linux zur Verfügung und zwar kostenlos für 25 Akten. Jede weitere zeitlich unbegrenzt nutzbare Akte kostet 2,99 €. Spezielle Vorlagen für schematisierte Schriftsätze können fortgeschrittene Benutzer selbst einbinden, auf Wunsch übernimmt das die Advolux GmbH.

**Reduzierte Patentkosten:** Europäische Patente werden mit der Abschaffung der Pflicht zur Übersetzung in die für das Patent wesentliche Nationalsprache deutlich billiger. Das regelt das sogenannte Londoner Protokoll der Mitgliedstaaten.

**Fälschungen aussortieren:** Der Bundesgerichtshof verlangt, dass Online-Auktionshäuser das Anbieten von „offensichtlichen Plagiaten“ auf den Auktionsseiten verhindern. Das gilt aber nur, wenn die Kontrolle technisch möglich und zumutbar ist.

**Sperrung nach Hinweis:** Nur wenn ein Webhosting-Provider einen Hinweis auf eine „klare Rechtsverletzung“ erhalten hat, muss er den Zugang dazu sperren. Das entschied das Landgericht Karlsruhe.

**Leitfaden Online-Recht:** Für Juristen, Berater und Betreiber von Internetseiten haben Joerg Heidrich, Justiziar des Heise-Verlags, und Nikolaus Forgó von der Universität Hannover die Loseblattsammlung „Heise Online-Recht – Der Leitfaden für Praktiker und Juristen“ herausgegeben. Das zweibändige Werk kostet 99 € und ist über den Heise-Kiosk (*iX*-Link) zu bestellen.

**Thumbnail-Urteil:** Suchmaschinen verletzen die Rechte von Urhebern digitaler Bilder, wenn diese als Thumbnail angezeigt werden, ohne dass der Urheber dem vorher zugestimmt hat. Mit diesem Urteil hat Google für die Bildsuchmaschine einen schweren Rückschlag erhalten.

**Alte Telefone verboten:** Die Bundesnetzagentur hat mitgeteilt, dass ab 1. Januar 2009 wegen Lizenzwegfalls niemand mehr die schnurlosen, analogen Telefonsysteme CT1+ und CT2 benutzen darf. Verstöße werden mit Bußgeldern geahndet.

**Leitfaden zum Hackerparagrafen:** Der Branchenverband Bitkom hat einen kostenlosen Leitfaden für IT-Unternehmen und Mitarbeiter der Strafverfolgungsbehörden herausgegeben. Er soll helfen, strafbares Handeln nach dem umstrittenen „Hackerparagrafen“ zu vermeiden, und ist auf der Bitkom-Website herunterzuladen (*iX*-Link).

**Opt-Out genügt nicht:** In den allgemeinen Geschäftsbedingungen (AGB) darf dem Kunden nicht eine Einwilligung zur Datenverwendung für Werbezwecke et cetera mit dem Zusatz „ggf. streichen“ untergeschoben werden. Das entschied das Oberlandesgericht Köln.

*iX*-Link ix0807022

## Keine Markenverletzung im Internet ohne Inlandsbezug

Das Oberlandesgericht Düsseldorf (Urteil vom 22. April 2008, Az. I-20 U 140/07) hatte sich wieder einmal mit dem Umstand auseinanderzusetzen, dass das Internet keine Staatsgrenzen kennt, die geltenden Gesetze aber teilweise schon. Ein ausländisches Unternehmen war für eine Webseite verantwortlich, auf der eine Marke verwendet wurde, für die der Kläger nach deutschem Markenrecht Schutz genoss. Er scheiterte mit seiner Unterlassungsklage, obwohl eine Markenverletzung zunächst nahelag.

Die Richter wiesen die Klage ab, weil sie der Auffassung waren, dass die ausländische Webseite keinen „hinreichenden wirtschaftlich relevanten Inlandsbezug“, also keinen Bezug zu Deutschland hatte.

Das wäre aber Voraussetzung für einen Anspruch nach dem deutschen Markengesetz gewesen.

„Eine inländische Kennzeichenbenutzung kann nicht schon allein deshalb bejaht werden, weil Internetseiten von jedem Ort der Welt abrufbar sind“, so die richterliche Begründung. *Tobias Haar*

## Datenaustausch mit USA kommt

Nach Zustimmung der Bundesregierung Anfang Juni kann das Abkommen zwischen Deutschland und den USA zur Bekämpfung „schwerwiegender Kriminalität“ in Kraft treten, wenn in Kürze auch noch der Bundesrat zustimmt. Diese Zustimmung gilt als gesichert. Durch den Austausch von Informationen über Terrorverdächtige wollen die Verantwortlichen den internationalen Kampf gegen den Terrorismus verstärken. Daneben bildet er die Grundlage für einen automatisierten Austausch von Fingerabdruck- und DNA-Daten. Dazu soll das in der EU bereits praktizierte Hit/No-Hit-Verfahren zum Einsatz kommen. *T. H.*

## Urheberrecht virtuell

Auch vor virtuellen Welten wie Second Life macht das Urheberrecht nicht Halt. Dies hat das Landgericht Köln (Az. 28 O 124/08) entschieden. Nach Meinung der Richter kommt es grundsätzlich nicht auf die „Art der Festlegung des Werkes“ an, also ob dieses nur unter Zuhilfenahme von elektronischen Medien erstellt und angezeigt werden kann. Einzig entscheidend ist, dass es sich um eine durch Sprache, Bild und Ton vermittelte gedankliche Aussage handelt, die eine schöpferische Leistung darstellt. Im konkreten Fall ging es um ein virtuelles Modell des Kölner Doms in Second Life. Da es sich hierbei nicht um etwas Triviales handelte, kam dieser Schöpfung Urheberrechtsschutz zu. Das Urteil ist auch für Designer und andere wichtig, die oft im Auftrag Dritter Werbepräsenzen et cetera im Web schaffen. Ihnen steht derselbe Schutz wie in der Offlinewelt zu. *T. H.*

SOA Days: Serviceorientierung in der Praxis

# Bauchgrimmen

**Achim Born**

Den Schwerpunkt ihrer diesjährigen SOA-Tagung legte die Deutsche Post auf die Praxis. Namhafte Unternehmen melden erste Erfolge beim Einsatz serviceorientierter Architekturen.

Analysten und Berater betonen gern, dass es bei SOA in erster Linie ums Geschäft geht und nicht um Technik. Da war es konsequent, dass die Veranstalter der SOA Days, die Deutsche Post und die IBC Euroforum, nicht mehr, wie die Jahre zuvor, zwischen Geschäfts- und Technikaspekten trennten – die Teilung wirkte schon immer künstlich. Anders als in den Vorjahren bestimmten handfeste Erfahrungen der Unternehmen die Veranstaltung in Bonn.

„Bei SOA überwiegt der Business- und Nutzen-Aspekt“, bekräftigte Johannes Helbig, IT-Chef des Hausherrn. Vertreter namhafter Firmen unterstrichen in ihren Vorträgen die Einschätzung ihres Kollegen. Als IT-Leiter sehen sie sich gefordert, Geschäftsprozesse abteilungs- oder betriebsübergreifend zu unterstützen. Beispiel: das serviceorientierte Bestellmanagement der Post, das 1200 interne sowie bis zu 10 000 externe Nutzer versorgt und bis zu 10 000 Transaktionen stündlich bewältigt.

Michael Gorriz, IT-Verantwortlicher bei Daimler, verspricht sich von SOA mehr Effizienz. Sein Vorbild für das Architekturmanagement ist selbstredend der Fahrzeugbau mit seinem übergreifenden Modulmanagement. Gorriz präsentierte den Besuchern eine umfassende SOA-Blaupause sowie ein Architektur-Referenzmodell, das SAP-, JEE-, Mainframe- und .Net-Anwendungen einbindet. Erste Muster SOA-konformer Programme erstellte man für den Bestellanforderungsprozess sowie einen 2D/3D-Teilevisualisierungsdienst, den über 1000 Anwender in Entwicklung, Produktion, After Sales und Einkauf verwenden können.

Bereits auf zehn Jahre SOA-Einsatz blickt man bei der Credit Suisse zurück. Claus Hagen, der bei dem Schweizer Finanzdienstleister den Bereich Integrationsarchitektur leitet, plauderte aus dem Nähkästchen. Dem frühen Einstieg geschuldet ist die heute einigermaßen exotisch anmutende technische Basis des hauseigenen Information Bus: CORBA (Common Object Request Broker Architecture) und IBMs Messaging-Software MQ Series. Die kritische Masse, was Anzahl und Nutzung der Services angeht, sei längst erreicht. Gleichwohl nannte Hagen einige Punkte, die ihm Bauchschmerzen bereiten. Dazu zählen Servicedesign, Wiederverwendung von Services, Messgrößen für ihre Bewertung und die Kosten für die Qualitätssicherung Tausender Schnittstellen.

Laut Helbig sind diese Fragen bestenfalls theoretisch gelöst. Unter dem Dach des im Herbst 2007 gegründeten SOA Innovation Lab haben sich auf seine Initiative hin Anwenderunternehmen zusammengefunden, um die serviceorientierten Architekturen gemeinsam weiterzuentwickeln. In Arbeitsgruppen soll sich das Innovation Lab mit eigenständig ausgewählten Themen beschäftigen. Angelaufen sind bereits Projekte zu grundlegenden Aspekten. Dazu gehören beispielsweise die begriffliche Normierung, ein standardisiertes Trainingsprogramm sowie der Erfahrungsaustausch mit Technikanbietern. Weitere Projekte, etwa zu Modellierungsfragen und EAM Governance (Enterprise Architecture Management) sind geplant. (jd)

## Salesforce: Zugriff auf Google Apps

Auf seiner Kundenkonferenz in London stellte Salesforce die 26. Release (Summer 08) der Software-as-a-Service-Lösung (SaaS) für das Kundenmanagement vor. Diese Version soll unter anderem neue Kollaborationsfunktionen für die Module „Content“ und „Ideas“ umfassen. Für die Kommunikation mit Partnern und Kunden stellt sie entsprechende Portale bereit. Web-2.0-Techniken wie Tagging, Subscriptions und Empfehlungen (Ratings) sollen den Anwendern den Umgang mit Dokumenten und unstrukturierten Daten erleichtern.

Andere Komponenten hat Salesforce ebenfalls weiterentwickelt. SFA (Sales Force Automation) stellt beispielsweise Dashboards zur Verfügung und versorgt sie automatisch mit Updates. Der Benutzer kann in der Sommerversion mit Google-Apps (Büroprogramme, Kommunikations-Tools) arbeiten. Bislang gab es diese Integration lediglich mit Microsoft-Werkzeugen.

*Susanne Franke*

## Hybride Anwendungsentwicklung mit G5

Magic hat die neue Generation seiner Entwicklungsplattform eDeveloper (Arbeitstitel G5) vorgestellt. Damit erstellte sogenannte Rich-Internet-Anwendungen lassen sich auf herkömmliche Art sowie im SaaS-Modus (Software as a Service) einsetzen. Das aufwendige Trennen der Programme in die verschiedenen technischen Schichten (Client, Server, Kommunikation) erledigt das Werkzeug angeblich automatisch selbst. Da alle Applikationen auf einheitlichen Projektmetadaten basieren, muss der Entwickler Änderungen nur an einer Stelle durchführen, sie werden sofort in allen Betriebsformen wirksam. G5-Programme sind laut Magic kompatibel zu bestehenden eDeveloper-V10-Anwendungen. Letztere lassen sich daher, so der Anbieter, einfach für die Benutzung via Internet anpassen.

## Mehr Optionen für Spekulanten

Quicken, ein Programm für die private Finanzverwaltung, erhält mit der Version 9 einen überarbeiteten Wertpapierbereich inklusive Vermögens- und Risikomanagement. Mit dem Ersteren legt der Anwender vor dem Aktienkauf fest, welche Summe er einsetzen will, welches Risiko er einzugehen bereit ist. Danach lässt sich für jede Position ermitteln, wie viele Wertpapiere man kaufen kann. Das Risikomanagement vermittelt im Anschluss einen detaillierten Überblick über die Risikoentwicklung des Depots. Im Bereich der gewöhnlichen Finanzverwaltung ist das Programm vorbereitet für den einheitlichen europäischen Zahlungsverkehr (SEPA – Single Euro Payments Area). Außerdem hat Quicken 2009 das Onlinebezahlsystem Paypal integriert.




**Bessere Vorhersagen:** Als neues Modul seines Business Rule Management Systems JRules stellt Ilog den Studio Scorecard Modeler vor. Mit der Komponente können Anwender vor allem aus der Finanzwirtschaft statistische Scorecard-Modelle, die sie selbst erstellen, in JRules-basierte Entscheidungsdienste einbetten. Scorecards sind Instrumente zur Einschätzung von Risiken sowie für die Bewertung von Kundenverhalten.

**Mehr Durchblick:** Die Karlsruher AP AG hat ihre ERP-Software APplus mit einem Modul zur Unternehmenssteuerung ausgestattet. Das Managementsystem soll wesentliche Kennzahlen übersichtlich darstellen und Prozessketten über eine Drop-Down-Menüführung abbilden. Die Integration des Cockpits erfolgt auf .Net-Basis.

## Firefox 3 vor Vollendung

Mit drei Release Candidates Ende Mai und Anfang Juni haben die Entwickler des Webbrowsers Firefox die endgültige Freigabe ihrer Software vorbereitet, die für Mitte Juni erwartet wurde (nach Redaktionsschluss). Das genaue Datum gibt die Site „Spread Firefox“ (www.spreadfirefox.com) bekannt. Mit der Version 1.9 der Rendering Engine Gecko und der Einbeziehung der Grafik-Bibliothek Cairo soll der Seitenaufbau deutlich schneller als bislang erfolgen. Viele Kleinigkeiten sind hinzugekommen oder verändert worden. Das reicht von der überarbeiteten Adressleiste, die passende Sites zeigt, wenn man ein Stichwort eingibt, bis hin zu erweiterter SVG-Fähigkeit. Ein Klick auf das Favicon informiert über den Eigner der Site, und Surfer können einen unterbrochenen Download nach einem Neustart wieder aufnehmen. Außerdem enthält Firefox eine Bookmark/History-Verwaltung, die auf SQLite aufsetzt.



## XML-Framework Cocoon 2.2 mit Spring

Mit der Version 2.2.0 des XML-Web-Framework Cocoon haben sich die Entwickler vom mittlerweile stillgelegten Projekt Avalon abgewendet und setzen stattdessen auf das Java-Framework Spring 2.0. Anwendungen, die noch mit Avalon arbeiten, können nach wie vor auf Unterstützung bauen, aber die Entwickler raten von der weiteren Nutzung ab.

Neu in Cocoon 2.2.0 ist außer Spring die Einführung sogenannter Blocks (entspricht den Plug-ins in der Eclipse-Sprache), die die Modularisierung des gesamten Framework voranbringen soll. Die Module müssen jeweils als Java-Archiv (.jar) vorliegen. Mit dem Servlet-Service Framework 1.0.0 sowie Configuration 1.0.2 hat das Entwicklungsteam zwei Teilprojekte neu herausgegeben. Außerdem liegt eine Reihe von Blocks vor.



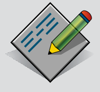
## Freie CFML-Engine in Vorbereitung

Die Schweizer Railo Technologies GmbH (www.railo-technologies.com) arbeitet gemeinsam mit den Entwicklern des freien Applikationsservers JBoss (www.jboss.org) an einer freien CFML-Engine (Coldfusion Markup Language). Sie wird in CFML geschriebene Webseiten in Java-Bytecode konvertieren. Dieser soll laut Railo in jeder Java-Servlet-Engine laufen. Fertig wird die Software jedoch erst Ende des Jahres.

Bis dahin wollen die JBoss-Entwickler den Kern des Applikationservers so erweitern, dass CFML-Programmierer Zugang zu Funktionen wie dem JBoss-Cache und -Messaging bekommen.



### KURZ NOTIERT



**Ex-Postnuke:** Auf der Grundlage des Content-Management-Systems Postnuke haben die Entwickler das Framework Zikula entworfen (zikula.org, zikula.de), das weniger CMS sein soll als vielmehr eine Bibliothek, die das Erstellen von Webanwendungen mit PHP (4.3 oder 5.x) erleichtert.

**Semantic Web:** Laut der Karlsruher Ontoprise unterstützt Version 5.1 ihres Ontobroker die Konvertierung zwischen den beiden W3C-Standards OWL und RDF sowie F-Logic und verfügt über eine bessere Leistung. Als Collaboration Server erlaubt die Software die verteilte Bearbeitung von Ontologien (www.ontoprise.de).

iX-Link ix0807028

## Facebook-API ist Open Source

Die Programmierschnittstelle Facebook Platform des (fast) gleichnamigen sozialen Netzes ist ein Jahr nach ihrer Vorstellung als Open Source nutzbar. Entwickler können ihre für Facebook programmierten Anwendungen auch für andere soziale Netze nutzen. Bestandteil des freigegebenen Pakets sind Parser für die Facebook Markup Language (FBML), die Anfragesprache FQL und die Javascript-Schnittstelle FBJS. Angesichts der von Google angeführten OpenSocial-Initiative erscheint dieser Schritt geradezu notwendig, wenn man dieser „offenen“ Konkurrenz gegenüber nicht Boden verlieren will.

Facebooks Charlie Cheever hatte zuvor verkündet, die Nutzung von Googles neuem sozialen Dienst Friends Connect abzuschalten. Die durch diesen Dienst mögliche Weiterverteilung von Benutzerdaten entspreche nicht Facebooks Nutzungsbedingungen. Diese verbieten es, Facebook-Daten so zu speichern, dass Dritte sie ohne schriftliche Vereinbarung nutzen können.

Wie Techcrunchs Michael Arrington wohl zu Recht vermutet (siehe *iX*-Links), dürfte es einen Zusammenhang mit dem von Facebook selbst am 9. Mai verkündeten Facebook Connect geben, das es ebenfalls erlaubt, Benutzerdaten über die Grenzen der einzelnen Anwendung hinaus zu transportieren.



## Videos ziehen neue Internet-Nutzer an

Laut der ARD/ZDF-Onlinestudie 2008 sind mittlerweile 42,7 Millionen Erwachsene in Deutschland online – 1,9 Millionen mehr als im Vorjahr. Dazu beigetragen hat die steigende Nachfrage nach multimedialen Anwendungen. So rufen 55 Prozent der Internet-Nutzer Videos ab und schauen live oder zeitversetzt Fernsehsendungen. Diesen Trend spiegelt die Tatsache wider, dass 70 Prozent der Befragten über einen DSL/Breitband-Anschluss verfügen (2007: 59 Prozent). Prozentual leicht gesunken ist die Nachfrage nach Audiodateien: 35 % im Vergleich zu 37 % im Vorjahr.

Insgesamt wurden im Rahmen der bundesweiten Studie im März/April 1802 Erwachsene befragt. Die höchsten Zuwachsraten hat man bei den 60- bis 79-Jährigen festgestellt: 29,2 Prozent der sogenannten „Silver Surfer“ bewegen sich inzwischen im Netz.



## Ruby on Rails 2.1 und Ruby 1.8.7

Unter anderem einen einfacheren Umgang mit Zeitzonen bietet Version 2.1 des Programmier- und Laufzeit-Framework Ruby on Rails (rubyonrails.org/down). Daneben wurden die Veränderungsverfolgung und das Caching verbessert. Die aktuelle Version, die sechs Monate nach dem Erscheinen von Ruby on Rails 2.0 veröffentlicht wird, ist ab sofort verfügbar. Die Macher berichten, dass rund 1400 Mitwirkende über 1600 Patches und Verbesserungsvorschläge eingereicht hätten, von denen sehr viele umgesetzt wurden.

Zeitgleich zur neuen Framework-Version wurde auch die neueste produktive Version der zugrunde liegenden Programmiersprache Ruby online gestellt (www.ruby-lang.org), in die schon einige Features der geplanten Version 1.9 eingeflossen sind. Unter anderen können Enumerationen jetzt Rückgabetyp von Objekten sein, weitere aus der geplanten Version 1.9 rückportierte Fähigkeiten sind die Securerandom-Library oder SSL/TLS für die Net/SMTP-Bibliothek.

Bis einschließlich Version 1.8 basiert Ruby auf dem in C geschriebenen Interpreter von Yukihiro „Matz“ Matsumoto, Version 1.9 arbeitet mit einer Bytecode-Maschine namens YARV (Yet Another Ruby Virtual Machine).

iX-Link ix0807028

## Markt für Geoinformationen – Wunsch und Wirklichkeit

Eine Studie der Micus Management Consulting GmbH sieht für deutsche Firmen erhebliche Marktchancen im internationalen Markt für Geoinformationen. Hintergrund ist die erhöhte Aufmerksamkeit für dieses Marktsegment durch viel beachtete Anwendungen wie Google Earth und Microsofts Virtual Earth. Der Zugang zu diesen neuen Märkten werde durch branchenorientierte Lösungen erleichtert.

Der deutsche Geoinformationsmarkt habe 2007 ein Volumen von 1,5 Milliarden Euro erreicht und sei seit 2000 um etwa 50 % gewachsen. Ein großer Teil des Umsatzes sei durch Navigation und mobile Services generiert worden; allein die Verkäufe von mobilen und in Kfz installierten Geräten betrugen im vorigen Jahr rund 1 Milliarde Euro. Auffallend sei, so die Studie, dass öffentliche Geodaten zunehmend durch das günstigere Angebot privater Dritter ersetzt würden. Micus hat die Daten europäischer und globaler Geoinformationsmärkte in der Internetanwendung Geo Business Maps dargestellt, auch die Studie steht zum Download bereit.

Deutlich skeptischer sehen Forscher von der TU Wien die Chancen in Sachen Geodaten für europäische Firmen. Ein Tagungsbeitrag verweist darauf, dass seit zehn Jahren zweistellige Zuwachsraten vorausgesagt werden. Diese seien auch in manchen Ländern erreicht worden – aber nicht in Europa. So seien in den USA mittlerweile die Umsätze mit Geoinformationen 10-mal so hoch wie in Europa.

Eine Ursache: Bereits um 1980 sind in den USA die Daten der topografischen 50000er-Karten und der Strassengraph mit Adressen frei verfügbar geworden, eine kommerzielle Nutzung ist zugelassen. In Europa dagegen seien zwar oft Daten sogar besserer Qualität vorhanden, aber nicht für kommerzielle Nutzungen verfügbar.

*iX-Link ix0807028*




## Stand von Microsofts OOXML

Die Standardisierungsgremien ISO und IEC werden die geplante Norm ISO/IEC DIS 29500 – Microsofts OOXML – zunächst nicht veröffentlichen, da vier Mitgliedsstaaten Einsprüche gegen die Normierung erhoben haben.

Fast zur selben Zeit hat Microsoft ein Entwicklungskit für OOXML angekündigt. Über das Download Center des Herstellers (siehe *iX*-Link) können Entwickler die Version 1 des Solution Developers Kit für die Erstellung von Open XML-Formate nutzende Client-Server-Anwendungen herunterladen.

Mit dem für 2009 erwarteten nächsten Service Pack ihres Office-Pakets will Microsoft anbieten, Dokumente im konkurrierenden Open Document Format (ODF) zu speichern. Die Redmonder wollen außerdem der für ODF als Standard zuständigen OASIS beitreten, um an der Entwicklung von ODF teilhaben zu können.

## *iX*-Veranstaltungen

www.ix-konferenz.de

Dass wir die Zusammenarbeit mit unserem langjährigen Autor Holger Schwichtenberg intensiviert haben, wurde bereits im letzten Heft erwähnt – aus Platzgründen allerdings nur in knappen Worten.

Darum jetzt noch einmal etwas ausführlicher: Neben Umsteiger-Workshops von Net 2.0/3.0 auf Version 3.5 und Visual Basic 6.0 zu 7.0 sind für viele sicherlich die stufenweise buchbaren Seminare zu **.Net-Web-** respektive **.Net-Desktop-Anwendungen** interessant. Unter der Bezeichnung „Camp“ dauern sie jeweils fünf Tage. Man kann aber auch nur die ersten beiden Tage für einen intensiven Einstieg buchen oder die letzten drei, wenn man sich das zutraut – Details sind wie immer auf der Konferenz-Website www.ix-konferenz.de zu finden, Start ist im Juli.

Über die schon in den Vorjahren erfolgreichen Veranstaltungen mit dem **C++-Guru Scott Meyers** berichteten wir an dieser Stelle bereits. Nicht unerwähnt bleiben soll, dass der Frühbucherrabatt nur noch bis zum 8. Juli gewährt wird.

Das in der letzten Ausgabe angekündigte neue Event-Format **Roadshow** hat sich schnell entwickelt, beim Schreiben dieser Zeilen sind bereits vier davon geplant. Auch hierzu finden sich Details auf www.ix-konferenz.de.



**Frühbucherrabatt bis 8. Juli: Workshops mit C++-Guru Scott Meyers**

Werden IPv4-Adressen zu Spekulationsobjekten?

# Adressenhandel

**Monika Ermert**

Die Mitglieder des Réseaux IP Européens (RIPE), die sich im Mai in Berlin trafen, und der vier anderen regionalen Internet Registries diskutieren derzeit darüber, ob sich das Entstehen eines Schwarzmarktes für IPv4-Adressen zugunsten eines offenen, kontrollierbaren Marktes verhindern lässt.

Internet-Adressverwalter verbreiten eine zunehmende Hektik. Das Aus der IPv4-Adressreserven sei in greifbare Nähe gerückt, dennoch komme IPv6 kaum voran. Wie sich eine Verknappung von IPv4-Adressen auswirkt, darüber gibt es viele Spekulationen. Unter anderem scheint ein Handel mit der begrenzten Ressource unvermeidlich zu sein.

IP-Adressen waren einmal eine öffentliche, freie Ressource. Mit der vermehrten Weitergabe oder gar dem Verkauf – selbst bei Ebay tauchten die Adressen schon auf – ist diese Idee infrage gestellt. „Verhindern kann man den Handel nicht,“ so Gert Döring, Vorsitzender der Adress Policy Working Group beim RIPE und seit Jahren Berichterstatter zur Entwicklung von IPv6-Routen. 1000 IPv6-Routen sind inzwischen in der Routing-Tabelle verzeichnet. Im Vergleich zum Wachstum der IPv4-Routen ist das allerdings nach wie vor sehr bescheiden.

Schon jetzt wechseln IPv4-Adressblöcke den Besitzer, und zwar bei Firmenaufkäufen oder Zusammenschlüssen. Daher beklagt man beim RIPE Network Communications Center (RIPE NCC), dass es manchmal schwierig sei, auf dem Laufenden zu bleiben, wo IP-Adressen hinwandern. Provider-unabhängigen Adressraum (PI), den ein Provider für einen Endkunden beantragt und lediglich weiterreicht, gibt es künftig nur noch bei klarer vertraglicher Regelung. Endkunden, die solchen gut fürs Multihoming geeigneten Adressraum benötigen, müssen entweder einen Vertrag mit der Local Internet Registry (LIR), also ihrem ISP, haben oder aber direkt mit dem RIPE NCC.

Noch eine weitere Regelung soll ein Chaos der Routen verhindern, wenn Adressen gehandelt werden: Zertifikate. Das RIPE NCC beginnt derzeit testweise, Adressressourcen PKI-Zertifikate zuzuordnen. RPKI soll in Zukunft intelligentes Filtern erlauben, um etwa das Hijacking von Routen zu verhindern. Für die Netzbetreiber selbst erlaube RPKI, klar nachzuvollziehen, ob jemand Inhaber von Adressressourcen ist, die er gerne geroutet haben will. ARIN und LACNIC haben die RPKI-Entwicklung besonders vorangetrieben.

Beim ARIN, der für Nordamerika zuständigen Adressvergabestelle, will man dem Handel nicht so liberal begegnen wie beim RIPE. Solange es noch „frische“ IPv4-Adressen gibt, soll der Handel ganz unterbleiben. Sind die letzten Reserven der Regionalen Internet Registries (RIRs) aufgebraucht, will ARIN den Handel kontrollieren. Nur Adressweitergaben, die ARIN absegnet, sollen laut dem aktuellen Regelentwurf zulässig sein. Beim RIPE bevorzugen viele Experten einen offenen Handel, der es der Adressverwaltung erlaubt, ihre Datenbanken aktuell zu halten, gegenüber einem in den Untergrund abwandernden Schwarzmarkt. Ausgerechnet große Telecom-Unternehmen und deren Verband, ETNO, warnen jedoch vor einer Liberalisierung. Diese Unternehmen sind allerdings bestens mit IPv4-Adressen versorgt.

Eine weitere Komplikation, mit der die Adress-Experten hadern, beseitigen alle Absicherungsmaßnahmen wie Verträge und RPKI aber nicht: das explosionsartige Wachsen der Routingtabellen. Derzeit bevölkern vor allem die rasch wachsenden IPv4-Einträge die Tabellen. Mit dem für menschliches Verständnis praktisch grenzenlosen IPv6-Adressraum verschärft sich das Problem aber in Zukunft noch. Mancher rät zu einer konservativen Vergabe kleiner PI-Blöcke, andere möchten denen, die ihren Adressraum unnötigerweise stückeln und damit die Tabellen aufblähen, auf die Finger klopfen. Ein technischer Ansatz ist die Trennung von Endpoint Identifier (EID) und Resource Locator. Während Endpunkte immer die gleichen EID-Adresse behalten, können die Resource-Locator-Adressen gewechselt werden. Auch Multihoming wäre damit möglich. Noch ist nicht absehbar, ob das unter dem Titel LISP (Locator Identifier Split) bei der Internet Engineering Task Force entwickelte Protokoll sich durchsetzen wird. (un)

## Abhöraffäre beeinträchtigt das Image der Telekom

Das systematische Ausspionieren von Telekommunikationsanwendern kann für die Telekom unliebsame Folgen haben. Ein Drittel der Kunden will deswegen „bestimmt“ oder „wahrscheinlich“ zu einem anderen Anbieter wechseln. 23 % „überlegen noch“, ob sie vielleicht wechseln wollen. Dies sind die Ergebnisse einer repräsentativen Umfrage des Kölner Marktforschungsinstituts Psychonomics im Auftrag der Wirtschaftswoche. Auch habe fast jeder zweite Befragte das Vertrauen in die Telekom verloren und fürchte um die Sicherheit der Kundendaten. Schlussendlich hat sich laut Umfrage das ohnehin nicht besonders gute Image der Telekom weiter deutlich verschlechtert.

## Europäische Kommission will IPv6 fördern

Die EU-Kommission hat Ende Mai einen Aktionsplan für IPv6 verkündet. In erster Linie will die Behörde selbst mit gutem Beispiel vorangehen und die eigenen Dienste auch über IPv6 erreichbar machen. Den Mitgliedsstaaten will sie entsprechende Selbstverpflichtungen nahelegen. IPv6 soll bei allen Ausschreibungen zu einem zwingenden Standard werden. Auch thematische Netze von Webangeboten, die bereits beide Sprachen sprechen, will die Kommission zusammenschweißen. Angefragt hat ein Vertreter der Kommission schon einmal bei Google. Der Suchmaschinenbetreiber hat im März als einer der ersten großen den Sprung ins kalte Wasser gewagt. Seither ist unter ipv6.google.com eine IPv6-Variante der Suchmaschine erreichbar. Bei den Suchergebnissen heißt es allerdings dann wieder zu fast hundert Prozent: kein Anschluss unter dieser Nummer. *Monika Ermert*

## iPhone: Mehr Technik für weniger Geld

Auf Apples World Wide Developer Conference (WWDC) hat Steve Jobs Anfang Juni den Nachfolger des bisherigen iPhone vorgestellt. Er funkt erwartungsgemäß mit UMTS und GSM – noch vor einem Jahr hatte Apple UMTS wegen der dadurch verkürzten Akkulaufzeiten für nicht sinnvoll erklärt. Nun heißt es, die neue Version des Smartphone biete eine „Sprechdauer von fünf Stunden“ im 3G-Netz.

Hinzugekommen ist auch ein GPS-Modul; das integrierte Google Maps zeigt mit seiner Hilfe die aktuelle Position des Geräts als Punkt auf der Landkarte an. Bei der Software gab es einige notwendige Verbesserungen. Bereits bekannt war die Anbindung an Microsofts Exchange Server, die das iPhone für Geschäftskunden attraktiver machen soll. Im täglichen Einsatz hilfreich dürfte die Suche in Kontakten sein (bislang war nur Blättern möglich) sowie das Markieren und Löschen oder Verschieben mehrerer Mails in einem Rutsch.

Erstmals lassen sich auf dem iPhone 2.0 Anwendungen von Drittanbietern installieren, jedoch nur über Apples iTunes-Shop. Auf der WWDC stellten Entwickler einige Programme vor, die zwischen 0 und 10 US-Dollar kosten sollen. Auch über den Preis will Apple den Reiz für größere Käuferschichten erhöhen. Die Preise liegen jeweils 200 US-$ unter den bisherigen, was beim Einstiegsmodell einer Halbierung gleichkommt: Die 8-GByte-Variante wird in den USA für 199 US-$ verkauft werden. Doppelt so viel Speicher lässt sich Apple mit weiteren 100 US-$ bezahlen. Preise für Europa waren bei Redaktionsschluss noch nicht bekannt.

## *iX*-Umfrage: Jeder Zweite schon von Viren betroffen

Die Bewertung der Antworten auf die Frage, ob der Arbeitsplatz-PC schon einmal von einem Virus verseucht war, hängt ein bisschen vom Typ ab. Betrachtet man ein zu 50 Prozent gefülltes Glas als halb voll oder als halb leer? Denn knapp die Hälfte wusste vom Befall des eigenen Rechners zu berichten – wenigstens hatte bei den meisten der Virenscanner früh genug Alarm geschlagen. Die genauen Zahlen sind der nebenstehenden Grafik zu entnehmen.

**Haben sich auf Ihrem Arbeitsplatzrechner schon einmal Viren oder andere Schadprogramme eingenistet?**

| Antwort | Anteil |
|---|---|
| Nein – zumindest schlug mein Virenscanner noch nie Alarm. | 39 % |
| Nein – und ich sehe auch künftig keinen Anlass, einen Virenschutz zu installieren. | 14 % |
| Ja – aber mein Virenscanner hat rechtzeitig gewarnt. | 40 % |
| Ja – und ich habe es erst durch den angerichteten Schaden bemerkt. | 7 % |

Gesamtstimmen: 740 (gerundet)

In der nächsten Umfrage geht es um die in der Firma eingesetzten Webserver.

## Kritik an IP-Bitstrom-Entgelten

Die Bundesnetzagentur hat im Mai die Preise für „entkoppelte“ DSL-Zugänge (IP-Bitstrom) festgelegt, die keinen Festnetzanschluss voraussetzen. Der monatliche Grundpreis für die Miete des Vorleistungsproduktes beträgt 19,05 Euro je Anschluss bei einer durchschnittlichen Nutzung von 50 kBit/s. Falls Endkunden über einen IP-Bitstrom künftig höhere Datenmengen (durchschnittlich 75 kBit/s) in Anspruch nehmen, beläuft sich das Entgelt für die monatliche Überlassung auf 20,05 Euro. Bleibt neben dem DSL-Anschluss der herkömmliche Telefonanschluss erhalten, fallen 8,55 Euro für den IP-Bitstrom an die Telekom an. In solchen Fällen wird dann aber zusätzlich der volle Endkundenpreis für den Telefonanschluss fällig. Für die Einrichtung des IP-Bitstrom-Zugangs steht nun ein Einmalentgelt in Höhe von 45,09 Euro für die reine Datenleitung und 56,47 Euro für die Variante mit Beibehaltung des Telefonanschlusses fest.

Anlässlich der Bekanntgabe ließ sich Bundesnetzagentur-Präsident Matthias Kurth zitieren: „Die genehmigten Entgelte für den IP-Bitstrom-Zugang fügen sich in konsistenter Weise in das Preisniveau der bisher schon verfügbaren Vorleistungen, insbesondere für die Teilnehmeranschlussleitung, ein.“ Er räumte allerdings ein, dass man es mit dem jetzigen Beschluss, der unter anderem Vorgaben der EU nachkam, nicht allen recht machen könne. Außer der Telekom übten weitere TK-Anbieter mit eigener Infrastruktur Kritik. Als „Schlag ins Gesicht des Infrastrukturwettbewerbs“ bezeichnete Breko-Präsident Peer Knauer die Entgelt-Festsetzung für die Basisvariante. Man hatte sich einen höheren Erlös erhofft (*iX* 6/2008, S. 36).

Der Versatel-Chef sieht insbesondere die Investitionen der im Bundesverband Breitbandkommunikation (Breko) organisierten Teilnehmernetzbetreiber gefährdet. Unternehmen wie Netcologne in Köln oder M-Net in München haben damit begonnen, einzelne Gebäude mit Glasfaserleitungen anzubinden, die Endverbrauchern Übertragungskapazitäten bis zu 100 MBit/s zur Verfügung stellen. Anbieter von Breitbandanschlüssen auf Basis von IP-Bitstrom würden dagegen auf den Aufbau eines eigenen Anschlussnetzes verzichten. „Nachdem die Bundesnetzagentur deutlich zu niedrige und inkonsistente Vorleistungskonditionen für infrastrukturlose Anbieter festgelegt hat, wird es immer unattraktiver, den auf der überteuerten Teilnehmeranschlussleitung basierenden Netzausbau fortzusetzen“, heißt es weiter in der Verbandsstellungnahme.

Die Bundesnetzagentur sieht das naturgemäß ein wenig anders und verweist auf die Ergebnisse von „sehr umfangreichen, unter Einbezug einer aufwendigen Marktabfrage durchgeführten Prüfungen“. Allerdings unterstellt man dabei, dass ein Unternehmen schnelle Leitungen auf Basis eigener Infrastruktur realisiert und dafür vor allem auf die „letzte Meile“ der Deutschen Telekom zurückgreift. Die Kosten dafür sollen nach Erkenntnis der Regulierungsbehörde niedriger liegen als diejenigen eines Konkurrenten, dessen Geschäftsmodell auf IP-Bitstrom ohne eigenständigen Telefonanschluss aufbauen wird.

*Achim Born*

### KURZ NOTIERT

**Exklusiv:** Yahoo und Netlog sind eine mehrjährige Partnerschaft eingegangen. Yahoo wird zum exklusiven Online-Werbungsvermarkter der Social-Networking-Plattform. Netlog erreicht hierzulande mit seinem Angebot monatlich 1,3 Mio. Anwender, die durchschnittlich 177 Minuten mit dem Angebot verbringen.

**Querschläger:** Spammer missbrauchen verstärkt existierende Absenderadressen. Laut Eleven hat sich allein im März 2008 das Volumen unerwünschter Spam-Rückläufer (Bounces und anderer „Backscatter“) verdreifacht.

## Acrobat 9 mit nativer Flash-Unterstützung

Über den integrierten Support für Flash können Anwender von Acrobat 9 Flash-Player-kompatible Anwendungen direkt in PDF-Dokumente einbinden. Inhalte unterschiedlichen Formats – von Audio- und Video-Dateien bis zu 3D-Objekten – lassen sich zudem in einem einzigen Dokument, dem PDF-Portfolio, zusammenführen. Für die anschließende Darstellung der Inhalte kann man zwischen diversen Layouts wählen oder ein eigenes Portfolio-Layout mit den gewünschten Navigationsmöglichkeiten auf Flash-Basis definieren.

Anwendern, die mit anderen gemeinsam online PDF-Dokumente bearbeiten wollen, bietet Adobe Systems einen neuen kostenlosen „Hosted Service“ an. Über Acrobat.com können sie PDF-Dokumente in Echtzeit steuern, Daten über Formulare erfassen, in Dateien speichern und austauschen. Voraussetzung für die Darstellung ist der kostenlose Acrobat Reader 9. Weitere Anwendungen von Adobe erlauben unter anderem Chatting sowie Video- und Audiokonferenzen.

Acrobat 9 (www.adobe.de/acrobat) gibt es in verschiedenen Ausführungen für Windows sowie eine Pro-Version für Mac OS X. Die Preise inklusive Mehrwertsteuer liegen zwischen 420 und 980 €, wer eine frühere Version besitzt, bekommt günstigere Update-Preise.

Gleichzeitig mit der neuen Version der PDF-Software hat Adobe angekündigt, Acrobat 9 Pro in die Creative Suite 3.3 zu integrieren. Die kommende Version der Sammlung von Publishing-Programmen wird zudem neue Versionen von Dreamweaver, Fireworks und Soundbooth enthalten. Public-Betaversionen sind als kostenlose Downloads über www.labs.adobe.com verfügbar. Interessierte können die Software 48 Stunden lang testen, wer bereits im Besitz von CS 3 ist, kann die Programme bis zum Erscheinen der neuen Version von Creative Suite ausprobieren.

iX-Link ix0807033

## Grafik-Benchmark SPECviewperf 10 für Linux und Unix

Die Standard Performance Evaluation Corp. (SPEC) hat die Version des Grafik-Benchmarks SPECviewperf für Linux und Unix zum kostenlosen Download freigegeben (www.spec.org/gwpg/downloadindex.html). Der Viewperf misst die Performance von OpenGL-Anwendungen. Zu den neuen Funktionen zählen unter anderem die Unterstützung von Prozessoren mit mehreren Kernen sowie von Full-Scene Anti-Aliasing (FSAA), das die komplette Szene und nicht nur die Kanten glättet. Außerdem misst der Benchmark die Effektivität grafischer Subsysteme, wenn Anwendungen in mehreren Threads laufen. Im Interesse kleinerer Downloads hat die SPEC den Benchmark außerdem in der neuen Version von den Testdateien, den sogenannten Viewsets, getrennt.

iX-Link ix0807033

## Grafik-Toolkits für .Net

Ilog (www.ilog.com) hat neue Versionen ihrer Grafik-Toolkits Diagrammer und Gantt vorgestellt, die Microsofts WPF-Schnittstelle sowie ASP.Net Ajax unterstützen. Entwickler können damit schnell interaktive grafische Anwendungen für das Web erstellen und dabei auf WPF-Template-Funktionen und die Graph-Layout-Bibliothek zurückgreifen. Anwender von Diagrammer for .Net 1.5 können unter anderem Visual Studio, Expression Blend, XAML, Videos und Animationen nutzen. Eine Einzelplatzlizenz von Diagrammer kostet 2500 €, die für Gantt for Net 3.5 1500 €.

iX-Link ix0807033

## Windows-Unterstützung verbessert

Novell hat mit dem jetzt freigegebenen Service Pack 2 seiner Linux-Distribution für den Unternehmenseinsatz neben Verbesserungen beim Clustering unter anderem das Zusammenspiel mit Windows-Systemen überarbeitet. So kann die aktualisierte Xen-Version 3.2 nun Windows Server 2003 und 2008 beherbergen. Der Kernel bietet einen Treiber auch für den schreibenden Zugriff auf NTFS-Dateisysteme. Openoffice 2.4 spendierten die Entwickler neben Feinschliff am VBA-Modul der Tabellenkalkulation unter anderem eine Vorabversion des OOXML-Konverters. Darüber hinaus kündigte Novell für seine Enterprise-Linux-Familie ein Subscription Management Tool an. Es soll ähnlich wie Red Hats Satellite Server als Paket-Proxy das Update-Management in größeren Umgebungen an einer Stelle konzentrieren, die sich sicherheitstechnisch besser überwachen lässt.

## Virtuelle Abhängigkeiten visualisiert

Smarts Application Discovery Manager (ADM) von EMC erkennt in der Version 6.0 nun auch Applikationen und deren Abhängigkeiten in virtualisierten VMware-Umgebungen. Die Software überwacht mithilfe der Komponente Virtual Listener automatisch Konfigurationsänderungen sowie virtualisierte und physische Beziehungen in der Anwendungsinfrastruktur. Der Virtual Listener kann ohne Agenten virtuelle Maschinen inklusive der entsprechenden Applikationen lokalisieren, indem er über VMware vSwitch (Virtual Switches) die Ressourcennutzung der Anwendungen verfolgt. Dies ermöglicht den Administratoren, die Beziehungen und Abhängigkeiten zwischen den virtuellen Ressourcen sowie den laufenden Geschäftsapplikationen anzeigen zu lassen.

## IT-Infrastruktur ITIL-konform im Griff

Realtech ermöglicht mit der Version 6.2 des Administrationswerkzeugs theGuard Service Management Center neben einem ITIL-konformen Management heterogener IT-Infrastrukturen nun auch die Sicherung geschäftskritischer Prozesse. Hierzu verknüpft es Prozessinformationen betriebswirtschaftlicher Anwendungen (SAP etc.) mit den Statusdaten der IT-Infrastruktur. Der Einsatz von Korrelationstechniken unterbindet dabei die sonst üblichen Ereignisfluten. Auf Basis der Statusinformationen aller überwachten Komponenten berechnet das System die Verfügbarkeit und Performance und löst im Störungsfall Alarm aus. Die Anwendersicht auf einen Geschäftsprozess erfassen und beurteilen GUI-Roboter.

### KURZ NOTIERT

**Kostenbewusst:** Die Planview Opensuite for CMDBf ermöglicht die Nutzung aller dem Föderationsstandard folgenden Konfigurationsmanagementdatenbanken (CMDB), um ITIL-orientierte Initiativen in Sachen Service-Portfoliomanagement zu unterstützen. Die Integration über die Opensuite-Komponente erleichtert die automatische und genaue Einspeisung der Service-Topologie in Planview Enterprise SPM und schafft somit die Grundlagen zur Ermittlung der Gesamtkosten für jeden Service.

**Automatisiert:** EMC stellt mit Voyencecontrol 4.0 seine jüngste Lösung für automatisiertes Netzwerk-, Change- und Konfigurations-Management vor. Die modellbasierte Software erkennt automatisch Fehlkonfigurationen von Netzwerkgeräten verschiedener Anbieter und kann die konforme Konfiguration wiederherstellen. Zudem ist sie mit EMCs Resource-Management-Produkten aus der Smarts-Familie kombinierbar.

## Managementsoftware für drahtlose Netze

Die Funkwerk Enterprise Communications GmbH (FEC) bringt Wilma auf den Markt. Die WLAN-Managementsoftware unterstützt Administratoren beim Inbetriebnehmen von WLAN-Infrastrukturen und bei Wartungsaufgaben. Unter anderem inventarisiert Wilma die Access Points. Die Konfiguration der Netzwerkparameter erfolgt nicht geräteabhängig, sondern gruppenbasiert. Einmal zentral abgelegte Konfigurationsparameter lassen sich über das Unternehmensnetz auf neue Geräte übertragen. Die Managementsoftware übernimmt zudem das Einspielen von Firmware-Updates für alle Access Points oder für eine definierte Gerätegruppe. Darüber hinaus bekommt der Administrator regelmäßig alle Leistungsdaten wie die Auslastung des WLAN und der Access Points zu Gesicht, damit er Engpässen im Netzwerk vorbeugen kann.

FEC bietet die Software in zwei Varianten an: Die „Standard Edition“ für das Management von bis zu 30 Access Points kostet ab 599 Euro. Für größere Netze mit bis zu 200 Access Points gibt es die „Professional Edition“ ab 1999 Euro. Eine kostenlose Probeversion steht ebenfalls zur Verfügung.

## Unternehmens-Linux aufgefrischt

Am 21. Mai präsentierte Red Hat das zweite Update seines Enterprise Linux Version 5, RHEL 5.2 (Codename Tikanga). Vorab durchlief die Release ein zweimonatiges öffentliches Beta-Stadium. Damit sollen Kunden von massiven Verbesserungen bei der Hardware-Unterstützung und Qualitätssteigerungen profitieren.

Mehr als 300 RPM-Pakete erhielten neue Versionsnummern an dritter Stelle und verließen damit in ihrer Kennung den Hinweis auf ihre ursprüngliche Herkunft Fedora Core 6. Auch größere Updates sind präsent: Openoffice 2.3, Thunderbird 2.0 und Evolution 2.12 liefern funktionellen Anschluss an andere Distributionen. Der Instant Messenger *gaim*, seit April 2007 *pidgin* genannt, ist namentlich gemäß seinem Nachkömmling enthalten. Umgekehrt ist *evolution*, das *gaim* voraussetzt, weiterhin Bestandteil des Produkts. Firefox 3.0 Beta erfuhr den größten Versionssprung. Der ursprünglich als Voraussetzung für RHEL5 qualifizierte Hypervisor Xen ist in der Version 3.1.2 Bestandteil des Produkts. Das dafür von Red Hat entwickelte Werkzeug *virt-manager* trägt nun die Nummer 0.5.3 und wurde auf den Leistungsvorrat von *libvirt* 0.3.3 angepasst. Qemu, der als weitere Virtualisierungsschicht Unterstützung durch *libvirt* erfahren soll, ist weiterhin nicht in der Distribution vorhanden. Als unterstützte Hardware-Obergrenze für Virtualisierungsplattformen nennt Red Hat 64 CPUs und 512 GByte RAM.

Ergänzende Erweiterungen betreffen eine bessere Unterstützung von iSCSI, Infiniband und 10-GBit-Ethernet-Adaptern. Der von RHEL4.x her bekannte TFTP-Konfigurator *sys tem-config-netboot* zählt nun ebenfalls zur Distribution. Der Desktop zeigt Automount von CD/DVD- und von USB-Wechselmedien wieder an. Insgesamt verspricht der Hersteller Verbesserungen in allen Kerneinsatzbereichen: Virtualisierung, Desktop, Netzwerk, Storage & Clustering und Security.

*Fred Hantelmann*

## Hilfestellung per E-Mail

Der US-Hersteller Numara Software hat die Version 8.5 seiner Helpdesk-Software Numara Track-It auf den Markt gebracht. Zu den Neuheiten zählt das regelbasierte E-Mail-Anforderungsmanagement.

Trouble-Tickets lassen sich damit automatisch erstellen und anhand von definierten Kriterien – etwa Begriffen in der Betreffzeile – den entsprechenden Experten zuordnen. Nach Angaben des Herstellers soll der Speicherverbrauch beim Techniker-Client im Vergleich zur Vorgängerversion um mehr als 30 Prozent geringer ausfallen, im Serverbereich gar um fast 90 Prozent.




**Gesundheitswirtschaft:** Der Fachbereich Gesundheitswesen der FH Braunschweig/Wolfenbüttel (www.fh-wolfenbuettel.de) bietet erstmals zum Wintersemester 2008/2009 den Bachelor-Studiengang „Controlling und Informationstechnologie in der Gesundheitswirtschaft“ an. Die Bewerbungsfrist endet am 15. Juli.

**Für Ärzte:** Die Technische FH Berlin bietet ab dem Wintersemester 2008/09 einen postgradualen Master-Fernstudiengang „Medizinische Informatik“ an. In fünf Semestern können Ärzte den Studienabschluss „Master of Science“ erwerben. Weitere Informationen unter www.tfh-berlin.de/fsi.

## ITK-Branche bildet verstärkt aus

Die Zahl der neu abgeschlossenen Ausbildungsverträge in IT-Berufen ist im vergangenen Jahr im Vergleich zum Vorjahr um 9 % auf 14 856 gestiegen. Dies teilte der Branchenverband Bitkom mit. Das stärkste Wachstum verzeichnet das Berufsbild des Fachinformatikers mit einem Plus von 15 % (8674 Neuverträge) und das des Systemelektronikers mit einem Zuwachs von 4 % (2463 Neuverträge). Die Zahl der neuen Azubis in den kaufmännischen IT-Berufen hat sich dagegen mit knapp über 3700 im Vergleich zum Vorjahr kaum verändert. Allen Werbemühen zum Trotz ist der Frauenanteil unter den Ausbildungsanfängern seit 2002 von 14 % auf nur noch 9,1 % im Jahr 2007 gesunken. Alle Daten basieren auf Angaben der DIHK.

## Internationale Ausrichtung

HP Deutschland bietet einen neuen Bachelor-Studiengang an der Berufsakademie (BA) Baden-Württemberg an. Der Studiengang International Business Information Management (IBIM) ist eine Weiterentwicklung des Wirtschaftsinformatik-Studiums. Im Vergleich zu diesem befassen sich die neuen Inhalte vorrangig mit international orientierten Themen. Ein großer Teil der Vorlesungen wird dabei in englischer Sprache gehalten. Obligatorisch ist für alle Studierenden neben einem Auslandspraktikum bei HP auch ein Theorie-Semester im Ausland. Neben Englisch bietet das IBIM-Studium als zweite Fremdsprache Spanisch oder Chinesisch. Nähere Informationen unter www.hp.com/de/ausbildung.

## Höhere Gehälter

In der IT steigen die Gehälter so stark wie seit drei Jahren nicht mehr. Von 2007 auf 2008 erhöhten sich die Grundgehälter von Führungskräften um 3,2 % und die der Fachkräfte um 3,5 %. Zu diesem Ergebnis gelangt die jüngste Kienbaum-Studie „Vergütung von Führungs- und Fachkräften in der Informationstechnologie“, für die die Saläre von 6022 Positionen in 291 Unternehmen ausgewertet wurden. Demnach verdient ein Leiter der Informationsverarbeitung und Organisation im Jahr durchschnittlich 140 000 €. Die Jahresgesamtbezüge eines Leiters des IT-Managements betragen 125 000 €, gefolgt vom Leiter Anwendungsentwicklung mit 109 000 €. Unter den Fachkräften in der IT bezieht der Sicherheitsmanager mit 87 000 € im Durchschnitt die höchsten Gesamtbezüge. Die rangnächsten Plätze belegen Vertriebsmitarbeiter (83 000 €) und Gruppenleiter (80 000 €).



Sapphire 2008: Nicht viel Neues

# Interregnum

**Achim Born**

Mit ihrer Anwendermesse Sapphire legte SAP dieses Jahr einen Zwischenstopp in Berlin ein. Spektakuläre Neuigkeiten präsentierte man den Besuchern an den drei Tagen nicht. Sie erhielten lediglich ein Update auf die künftige Geschäfts- und Produktgestaltung, wobei manches im Nebulösen blieb.

Manchmal braucht es wenig zum Erfolg: Eine stringente Planung, eine ausreichende Finanzierung und die richtige Zusammensetzung des Teams. Wer dies beherzigt, erreicht sein Ziel mitunter ein oder zwei Jahre vor dem anvisierten Zeitpunkt. Dietmar Hopp, einer der SAP-Gründer, hat es mit der TSG 1899 Hoffenheim vorgemacht, die bekanntlich den Durchmarsch in die 1. Fußballbundesliga schaffte. Das Softwaregeschäft scheint ein wenig komplizierter zu sein. Zumindest gelang es SAP mit Business ByDesign nicht, dem Beispiel zu folgen: Die Markteinführung der Mietsoftware nach dem SaaS-Modell (Software as a Service) verzögert sich, wie man auf der Sapphire in Berlin erfuhr. Man habe gegenüber der ursprünglichen Planung ein wenig Geschwindigkeit herausgenommen, umschrieb der jetzige Ko-Chef und künftige Alleinvorstand Léo Apotheker beschönigend den revidierten Investitions- und Zeitplan.

Immerhin durften die Besucher die Mittelstandssoftware live erleben. Version 1.2 von Business ByDesign erhielt eine überarbeitete Benutzerführung, die gegenüber dem ersten Muster einen aufgeräumten Eindruck vermittelt. Neu ist auch das Speichermodell: Mit Blick auf Intels 64-Bit-Blades werden alle Transaktionsdaten im Hauptspeicher gehalten. Abfragen laufen nun nicht mehr direkt auf der Datenbank, sondern durch die hauseigene Suchmaschine TREX (Text Retrieval and information EXtraction). Damit fallen die Antwortzeiten für rund 90 % aller Transaktionen angeblich auf unter eine Sekunde.

Business ByDesign basiert bereits auf Technik, die in das Softwareangebot für SAPs Stammgeschäft erst noch Einzug halten soll. Insbesondere betrifft das Netweaver 7.1 einschließlich der im ESR (Enterprise Service Repository) verwalteten IT-Services und Prozessmodelle. Die Plattform bildet das Fundament neuer prozessorientierter Funktionen, die SAP auch der traditionellen ERP-Software spendieren will. Damit einher geht das Versprechen, dass die Release-Fähigkeit der auf Netweaver 7.0 (ohne ESR) basierenden mySAP Business Suite nicht gefährdet ist.

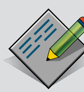
## Prozessentwurf in die Fachabteilung

Als erste Varianten der künftigen SOA-by-Design-Offerten nannte Henning Kagermann in seiner Eröffnungsrede kollaborative Lösungen zum Lieferantenmanagement und zur Produktentwicklung. Die Aussagen des langjährigen SAP-Chefs, der sich zurzeit die Regentschaft mit Apotheker teilt, blieben dazu jedoch ziemlich vage. Ausführlich sprach er dagegen über die grundsätzlichen Vorteile des neuen service- und prozessorientierten Designprinzips. Die Anwender erhalten vorgefertigte Prozessvorlagen und sollen ohne Programmierung Prozesse und Workflows entwerfen. Dabei helfen die Werkzeuge Netweaver Business Process Management (BPM) und Netweaver Business Rules Management, die man im dritten Quartal dieses Jahres an erste Kunden ausliefern will.

Kagermann erklärte, dass der Erfolg von Unternehmen künftig von kollaborativen Prozessen sowie der flinken Anpassung der Abläufe abhängen wird. Daher rechnet er damit, dass der Bedarf an klassischer ERP-Software zurückgeht. Und weil SAP für die prozessorientierten Lösungen eher die Fachals die IT-Abteilung begeistern möchte, sollen Dreibuchstaben-Akronyme wie CRM, ERP oder SCM bald der Vergangenheit angehören.

Eingedenk der Vielfalt – oder besser des Wirrwarrs – an Schlagwörtern und Abkürzungen, mit denen SAP & Co. die Anwender lange quälten, ist ein solcher Plan nur zu begrüßen. Ob er sich umsetzen lässt, steht auf einem anderen Blatt. Ebenso unsicher scheint, ob Kagermann noch die Früchte der von ihm angestoßenen Entwicklungen ernten kann. Denn fraglos ist sein Ko-Chef Apotheker, der ab Mai kommenden Jahres die Geschicke des Unternehmens alleine leiten soll, intern schon der starke Mann. Er will erst 2009 die Karten zu den weiteren Vorhaben aufdecken. Aus jüngsten Maßnahmen und seinen Äußerungen in Interviews lässt sich jedoch darauf schließen, dass er die Profitabilität von Entwicklungen in Zukunft schärfer kontrollieren will. (jd)

## KURZ NOTIERT



**Großes für Kleine:** SAPs Mittelstandsofferte Business All-in-One erhält CRM-Funktionen, die auf SAPs CRM 2007 basieren, einer Anwendung für Großunternehmen. Vorkonfigurierte Best Practices für durchgängige Abläufe für Vertrieb, Marketing und Service sollen die Einführung erleichtern.

**Eingekauft:** Netsuite, US-amerikanischer Anbieter von ERP-Software nach dem SaaS-Modell (Software as a Service), übernimmt Openair. Die ebenfalls in den USA ansässige Firma ist spezialisiert auf Lösungen für Professional Services Automation und Projekt-Portfoliomanagement. Zunächst verkauft Netsuite die Pakete einzeln, will aber die Openair-Software via Webservices in das eigene Angebot integrieren.

**BO-Integration:** Die auf der Sapphire vorgeführte Version 1.2 von SAPs Business ByDesign soll die offizielle Freigabe im Juli erhalten. Anfang kommenden Jahres steht Release 2.0 an, die den derzeitigen Funktionsumfang deutlich erweitern wird. Dabei bedient man sich aus dem Produktportfolio der aufgekauften Business Objects. So arbeitet die Xcelsius-Software hinter dem kommenden Verkaufs-Dashbord. Für Bilanzdokumente kommt Chrystal zum Einsatz, da hier pixelgenaue Darstellung gefordert ist.

**Ohne Geheimnisse:** Die On-Demand-CRM-Lösung Rightnow 08 verfügt über Chat-Funktionen, die Kundenrückmeldungen aus Online-Chats erfassen können sollen. In die letzte Edition hatte Rightnow bereits sogenanntes Topic Monitoring eingebaut, mit dem sich die Stimmungslage der Kunden angeblich automatisch analysieren lässt.

**Abgegeben:** Künftig wird die Desktop-Publishing-Produktlinie xMAM (XML-basierendes Media Asset Management) der Software AG primär von VVA Networks weiterentwickelt. Weiterhin darf der Dienstleister das Programm als OEM-Produkt unter eigenem Namen vertreiben.

**Kooperation:** SER und Recommind arbeiten künftig zusammen. Sie wollen die Content-Management-Lösung Doxis iECM mit der Mindserver-Technik kombinieren. Mit der Letzteren lassen sich assoziativ beispielsweise Dokumente, digitale Kundenakten und E-Mails durchsuchen.

## Zwei Netweaver-Tools für Prozessverarbeitung

Mit zwei neuen Werkzeugen für das Geschäftsprozessmanagement will SAP seine Technologieplattform Netweaver erweitern: Netweaver Business Process Management (BPM) und Netweaver Business Rules Management (BRM). Mit diesen Programmen sollen die Unternehmen ihre Geschäftsprozesse schneller an veränderte Rahmenbedingungen anpassen können. Erste Kunden werden die Tools voraussichtlich im dritten Quartal dieses Jahres ausprobieren dürfen.

Die Komponenten erfüllen laut SAP drei zentrale Funktionen: Mit dem Process Composer soll der Modellierer mithilfe der Business Process Modeling Notation (BPMN) Geschäftsprozesse erstellen. Dieses Werkzeug sowie ein Rules Composer zum Anlegen von Geschäftsregeln sind in die Eclipse-Entwicklungsumgebung integriert.

Mit dem Process Server, einer auf JEE basierenden Engine, kann er die Prozessmodelle direkt ausführen. Über den Process Desk schließlich erhalten die jeweiligen Nutzer eines Prozesses Zugang zu ihren Aufgaben. Dieses Hilfsmittel bietet Formulare, interaktive Bildschirme und sogenannte Collaboration Tasks zur Interaktion mit Kollegen und Prozessinstanzen.

## Herantasten an BPM

Einer Untersuchung namens „State of Business Process Management 2008“ zufolge haben Unternehmen trotz wachsenden Interesses an BPM noch Entwicklungsbedarf. Auf der CMMI-Skala (Capability Maturity Model Integration) der Studie befinden sich die meisten Firmen auf Stufe zwei. Es existiert noch keine vollständige unternehmensweite Prozessarchitektur, weder eine systematische Messung der Performance noch eine steigende Prozesseffizienz. Diese Maßnahmen müssen sie jedoch umsetzen, um die CMMI-Stufen drei, vier und fünf zu erklimmen. Die von der Software AG gesponserte Untersuchung haben die Marktforscher von BPTrends durchgeführt. Sie ist unter www.bptrends.com/surveys_landing.cfm verfügbar.




## SaaS von Strato

Jetzt mischt auch Strato im Markt für Unternehmenssoftware mit. Unter der Bezeichnung Strato Firmenportal (www.strato-pro.de) offeriert der Webhoster diverse Anwendungsfunktionen für kleine und mittlere Unternehmen nach dem SaaS-Betriebsmodell (Software as a Service). Das Angebot umfasst ein Content Management System (CMS) für Websites und Intranets, ein Dokumentenmanagementsystem (DMS) sowie ein Customer-Relationship-Management-System (CRM) mit den üblichen Funktionen. Die Programme basieren auf der Software von Siteforum. Für die Inbetriebnahme benötigt man lediglich einen Internetanschluss.



KURZ NOTIERT

**Auftrieb:** Der Softwaremarkt für Business Intelligence erreichte in Deutschland 2007 ein Gesamtvolumen von 689 Mio. Euro (+13,7 %). Das ermittelte eine Marktstudie des Business Application Research Center (BARC). Bis 2012 wird ein durchschnittliches jährliches Wachstum von 10 bis 12 % prognostiziert.

**Aufkauf:** Die Berliner PSI AG übernahm die Geschäftsanteile der F/L/S Fuzzy Logik Systeme GmbH mit Sitz in Dortmund zu 100 %. Die Software für Entscheidungsunterstützung und Prozessoptimierung der Dortmunder Firma sollen vor allem das PSI-Produktportfolio in der Produktionsleittechnik, Logistik und im Energie-Portfoliomanagement ergänzen.

**Im Plus:** Für das im März abgeschlossene Geschäftsjahr 2008 meldet IT-Management-Spezialist BMC ein Umsatzplus von knapp 10 % auf 1,73 Mrd. $. Die Lizenzeinnahmen betrugen im Betrachtungszeitraum 647,6 Mio. $ (+13,7 %). Mit Wartung wurden 967,7 Mio. $ (+5,3 %) und mit professionellen Dienstleistungen 116,3 Mio. $ (+26,7 %) erzielt. Der Nettogewinn stieg um rund 45 % auf 313,6 Mio. $.

**Gerangel:** Der Streit, ob Microsoft nun Yahoo kaufen soll, geht weiter. Carl Icahn – der beinharte Investor hält weniger als 5 % – strebt die Kontrolle über den Verwaltungsrat von Yahoo an. Falls ihm dies gegen den erklärten Widerstand von Yahoo-Boss und -Mitbegründer Jerry Yang gelingt, soll ein freiwilliger Verkauf an Microsoft für 34,375 $ pro Aktie eingeleitet werden. Die Gates-Firma hatte vor dem abrupten Ende der Übernahmegespräche zuletzt 33 $ pro Anteil geboten.

Standardsoftware in Deutschland

# Lohnende Geschäfte

**Achim Born**

Der Standardsoftware-Markt in Deutschland wuchs 2007 um über 6 %. Wie in der Vergangenheit war die Mehrzahl der 25 umsatzstärksten Anbieter größter Nutznießer und partizipierte überdurchschnittlich von dem Aufwärtstrend.

Der Trend aus 2005 und 2006 hat Bestand: Auch im vergangenen Jahr legten die hiesigen Geschäfte mit Standardsoftware deutlich zu. Dies betraf die Einnahmen mit Systemsoftware, Tools, Middleware und Datenbanksoftware (+5,3 %) sowie die Nachfrage nach Anwendungssoftware (+6,7 %). Insgesamt stieg in Deutschland der Umsatz nach Ermittlungen des Branchenverbandes Bitkom um rund 6,1 % auf 14 Mrd. Euro.

Aus der jüngsten Erhebung der Lünendonk GmbH geht hervor, dass die führenden 25 Anbieter im Betrachtungszeitraum Inlandsumsätze von zusammen über 7 Mrd. Euro erwirtschafteten. Ihre Einnahmen stiegen im Vergleich zum Vorjahr überdurchschnittlich um 7,3 %, sodass ihr Marktanteil erstmals bei 50 % liegt. Allerdings verzeichnen die in der Liste aufgeführten Unternehmen unterschiedliche Veränderungsraten zwischen plus 35 % und minus 32 %. Während zehn Firmen unter den Top 25 zweistellige Zuwachsraten erzielten, mussten vier von ihnen Umsatzrückgänge im Deutschland-Geschäft hinnehmen.

Die divergierenden Wachstumsraten wirken sich allerdings nur auf die Reihenfolge im Ranking aus. Die elf 2006 führenden Unternehmen sind aber auch 2007 unverändert auf den vorderen Plätzen zu finden. Microsoft, SAP und Oracle nahmen ihre angestammten Plätze auf dem Treppchen ein. Allein die Neuaufnahme der Datev (Platz 4) in die Riege der Standardsoftware-Anbieter brachte ein wenig Bewegung. Deutlich mehr Veränderung ist dagegen unter den in der hinteren Listenhälfte angeführten Firmen zu beobachten. So rutschte beispielsweise SoftM von Platz 12 auf Platz 19, während Sage von Rang 15 auf Rang 12 kletterte.

Aufnahme in die Lünendonk-Liste finden Unternehmen, die mehr als 60 % des Umsatzes mit Standardsoftware-Produktion, -Vertrieb und -Wartung erwirtschaften; das Ranking erfolgt nach Inlandsumsätzen. Dieser Systematik ist geschuldet, dass gerade exportstarke deutsche Softwarehäuser wie die Software AG in der Liste auf den hinteren Rängen auftauchen. Insgesamt verkauften die 14 Standardsoftware-Unternehmen aus der Liste, die ihren Hauptsitz in Deutschland haben, im vergangenen Jahr für über 9,2 Mrd. Euro Softwareprodukte ins Ausland. (WM)

**Top 25 der Standardsoftware-Anbieter**

| Rang | Unternehmen | Umsatz 2007 | Umsatz 2006 | Gesamtumsatz 2007[2] | Gesamtumsatz 2006[2] |
|---|---|---|---|---|---|
| 1 | Microsoft[1] | 2090 | 1990 | – | – |
| 2 | SAP | 2004 | 1907 | 10242 | 9393 |
| 3 | Oracle[1] | 620 | 527,5 | – | – |
| 4 | Datev | 614 | 585 | 614 | 585 |
| 5 | Infor[1] | 210 | 180 | – | – |
| 6 | Adobe[1] | 175 | 140 | – | – |
| 7 | CA Deutschland[1] | 127 | 133 | – | – |
| 8 | CompuGroup | 126,4 | 115,1 | 180,4 | 140,1 |
| 9 | Novell[1] | 126 | 110 | – | – |
| 10 | BMC[1] | 110 | 99,5 | – | – |
| 11 | PSI | 97,1 | 97 | 123,2 | 117 |
| 12 | SAS[1] | 96 | 90 | – | – |
| 13 | Sage | 76,5 | 56,6 | – | – |
| 14 | Software AG | 65,9 | 68,8 | 621,3 | 483 |
| 15 | Mensch und Maschine | 53,7 | 42,2 | 212,9 | 170,3 |
| 16 | Nemetschek | 53,6 | 45,7 | 146,2 | 107,5 |
| 17 | Beta Systems | 52,6 | 71,5 | 88,6 | 96,6 |
| 18 | Interflex | 52 | 49 | 73 | 70 |
| 19 | SoftM | 50,9 | 74,9 | 59,4 | 83 |
| 20 | Cognos | 50 | 42 | – | – |
| 21 | Schleupen | 49,6 | 48,2 | 49,6 | 48,2 |
| 22 | FJH | 45,8 | 42,2 | 61,3 | 56,9 |
| 23 | P&I | 43,2 | 41,7 | 54,5 | 50 |
| 24 | Proalpha | 37 | 33 | 46 | 41 |
| 25 | Simcorp | 37 | 36 | – | – |

[1]Umsatz teilweise geschätzt, [2]Hauptsitz in Deutschland — Umsatzzahlen in Millionen Euro

Quelle: Lünendonk GmbH, Mai 2008

## HP will EDS übernehmen

Hewlett-Packard bereitet den nächsten Mega-Deal vor. Für rund 13,9 Mrd. $ will man den IT-Service-Anbieter EDS kaufen. Die Aufsichtsräte beider Unternehmen haben der Übernahme einstimmig zugestimmt. Die Akquisition soll im zweiten Halbjahr 2008 abgeschlossen sein. Durch die Übernahme würde HP den Umsatz aus dem Geschäft mit IT-Dienstleistungen voraussichtlich mehr als verdoppeln; im Geschäftsjahr 2007 belief sich dieser auf 16,6 Mrd. $. Zusammen haben beiden Firmen einen Jahresumsatz von mehr als 38 Mrd. $ erwirtschaftet. Das weltweite IT-Dienstleistungsgeschäft ist äußerst heterogen. Selbst der führende Anbieter IBM erreichte der Gartner Group zufolge nur einen Anteil von 7,2 %. EDS, bereits die Nummer 2, kam gerade auf 3 % und HP als Nummer 5 erzielte 2,3 %. Im vergangenen Jahr konnten unter den führenden Anbietern nur IBM und Accenture überdurchschnittlich wachsen. Ob dies der neuen HP-EDS künftig auch gelingen kann, betrachten die Analysten mit Skepsis. Mit der EDS-Übernahme rückt HP im wichtigen Geschäft mit IT-Dienstleistungen zwar ein wenig näher an IBM heran. Auf der anderen Seite sind nach Ansicht von IDC-Mann Matthias Kraus beide Firmen dem Bereich des weniger lukrativen Infrastruktur-Outsourcing zuzuordnen. In der margenstärkeren Prozess- und Anwendungsberatung hat der Vorsprung von Accenture und IBM folglich zunächst einmal Bestand. Von Vorteil ist allerdings, dass HP durch EDS den dringend benötigten Zugriff auf größere Offshore-Kapazitäten erhält.

**Führende IT-Dienstleister 2007 weltweit**

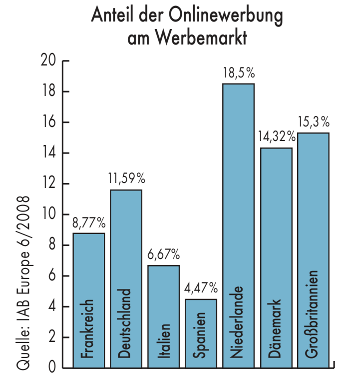
| Anbieter | Umsatz 2007 | Marktanteil | Wachstum |
|---|---|---|---|
| IBM | 54,148 | 7,2 % | 12,2 % |
| EDS | 22,130 | 3,0 % | 3,4 % |
| Accenture | 20,616 | 2,8 % | 19,7 % |
| Fujitsu | 18,620 | 2,5 % | 3,9 % |
| HP | 17,252 | 2,3 % | 8,1 % |
| CSC | 16,306 | 2,2 % | 7,7 % |
| übrige | 598,953 | 80,0 % | 10,7 % |
| gesamt | 748,025 | 100,0 % | 10,5 % |

Umsatzangaben in Milliarden Dollar

Quelle: Gartner, Mai 2008

## Onlinewerbung in Europa

Das IAB Europe (Interactive Advertising Bureau) stellte mit dem AdEx-Report ein detailliertes Zahlenwerk zu den Online-Werbeausgaben in Europa vor. Das Gesamtvolumen des europäischen Online-Werbemarktes belief sich danach im vergangenen Jahr auf 11,2 Mrd. Euro und lag 4 Mrd. Euro (40 %) über dem Vorjahresergebnis. Aufgrund des starken Wachstums konnte der europäische Online-Werbemarkt zum US-Markt aufschließen, der im gleichen Zeitraum nur um rund 26 % auf umgerechnet 14,5 Mrd. Euro zulegte. Der AdEx-Report beziffert den Anteil, den die Onlinewerbung am gesamten Werbemarkt in den Schlüsselmärkten einnimmt. In den Niederlanden beträgt diese Rate bereits 18,5 % und in Großbritannien 15,3 %. Hierzulande fließen knapp 11,6 % aller Werbeausgaben in den Onlinebereich. Erstmals bringt der Report eine Übersicht über die Ausgaben einzelner Branchen. Demnach haben 2007 die Branchen Unterhaltung/Freizeit, TK und Finanzen/Versicherungen am stärksten in Onlinewerbung investiert.




## Softwarepiraterie verlagert sich

Der Anteil unlizenzierter Software ist 2007 in Deutschland um einen Prozentpunkt auf 27 % zurückgegangen. Weltweit ist Softwarepiraterie dagegen deutlich auf dem Vormarsch. Der Anteil unlizenzierter Programme soll hier um drei auf 38 % gestiegen sein. Der Umsatzausfall für die Hersteller wird mit 48 Mrd. $ beziffert. Dies sind die Ergebnisse der jüngsten Untersuchung zur Softwarepiraterie, die IDC im Auftrag der Business Software Alliance (BSA) regelmäßig durchführt. Verantwortlich für die Zunahme sehen die Studienautoren insbesondere die wachstumsstarken Schwellenländer. Ihr Anteil am IT-Umsatz steigt überproportional, und somit führen ihre immer noch hohen Piraterieraten zu einem Anstieg des weltweiten Durchschnitts. Dieser Effekt lässt sich nicht dadurch kompensieren, dass Russland den stärksten Rückgang in Sachen Softwarepiraterie verzeichnet (von 80 auf 73 %). Ähnlich wie in Deutschland ist in vielen westlichen Staaten die Rate 2007 leicht gesunken. EU-weit verringerte sich der Anteil raubkopierter Software von 36 auf 35 %, die Schadenssumme sank trotz der Erweiterung des Staatenbundes um Bulgarien und Rumänien von 8,8 auf 8,5 Mrd. Euro (12,4 Mrd. $). Die BRIC-Staaten (Brasilien, Russland, Indien und China) machen nun etwa ein Drittel des weltweiten Umsatzausfalls aus (14,4 Mrd. $). In der Region Nordamerika soll er 9,1 Mrd. $ betragen.

**Top 6 der Piraterierate**

| | Land | Piraterierate | Umsatzausfall |
|---|---|---|---|
| 1 | USA | 20 % | 8,040 |
| 2 | China | 82 % | 6,664 |
| 3 | Russland | 73 % | 4,123 |
| 4 | Frankreich | 42 % | 2,601 |
| 5 | Indien | 69 % | 2,025 |
| 6 | Deutschland | 27 % | 1,937 |

Umsatzausfall in Milliarden Dollar

Quelle IDC/BSA, Mai 2008

## Betriebssysteme: Linux verdrängt Unix

Einer Prognose der US-Beratung Gartner zufolge nehmen Hersteller von Betriebssystem-Software heuer weltweit knapp 29 Mrd. $ ein. Dies entspricht einem Plus von 7,2 % gegenüber 2007 (knapp 27 Mrd. $). Für die kommenden Jahre erwartet Gartner ein unverändert hohes Wachstum. Spätestens 2012, so die Prognose, sollen die Einnahmen mit Betriebssystemsoftware die 37,5-Mrd.-$-Marke übersteigen. Gleichwohl wird nach Einschätzung der Analysten das Betriebssystem-Geschäft von einem grundlegenden Wandel ergriffen. Das Ersetzen von Unix durch Linux, neue Techniken wie Virtualisierung oder Multi-Core-Prozessoren und Maßnahmen gegen Produktpiraterie sollten nachhaltig das Marktgeschehen beeinflussen.

Bereits heute ist das Linux-Segment der am stärksten wachsende Server-Betriebssystemteilmarkt. Das quellcodeoffene Betriebssystem wird nach Gartner-Ansicht aufgrund des guten Preis-Leistungs-Verhältnisses, niedriger Betriebskosten und des breiten Angebots an Service-Offerten Unix weiter bedrängen. Techniken wie Virtualisierung gepaart mit Embedded-Applikationen sollen eines Tages die Betriebssystemssoftware von dem angestammten Middleware-Platz verdrängen. Multi-Core-Prozessoren führen wiederum zu einer neuen Lizenzgestaltung. Die durch Virtualisierung eingeleitete bessere Nutzung der IT-Ressourcen kann die traditionelle Betriebssystemnachfrage zusätzlich dämpfen. Hinzu kommt die vermehrte Nutzung von Mietsoftware in Unternehmen.

Die Gartner-Analysten empfehlen den einschlägigen Anbietern, sich in ihrer Produktpolitik auf diese Entwicklungen einzustellen. Erst einmal darf sich nach dem Urteil der Berater Microsoft über steigende Einnahmen freuen, da sich die Lebensspanne von Windows XP dem Ende nähert und Vista den Umsatz ankurbelt. Zusätzlich greifen die Maßnahmen im Kampf gegen Produktpiraterie. Allerdings trübt der Trend in den Schwellenländern, wo Behörden verstärkt auf Open Source und Linux setzen, den Ausblick auf das künftige Geschäft von Microsoft.

Sieben frei verfügbare Weblog-Systeme

# Liebes Tagebuch …

**Christoph Leisegang, Stefan Mintert**

Blogs waren zunächst als individuelles Webtagebuch verbreitet. Mittlerweile nutzen aber auch viele Firmen Weblog-Software und betreiben ein oder mehrere eigene Blogs. Während Privatpersonen gerne auf extern gehostete Software zurückgreifen, kommt für Firmen oft nur der Betrieb auf einem eigenen Rechner in Betracht.

Ein geeignetes Produkt für den Betrieb eines Blog auszuwählen, ist eine schwierige Aufgabe. Sie beginnt mit der Überlegung, welche Anforderungen die Software erfüllen soll. Ein zentraler Punkt sind die Systemvoraussetzungen, unter denen die Blog-Software läuft. Die im Rahmen dieses Artikels betrachteten Produkte benötigen entweder Java nebst einem Servlet-Container oder einen Webserver mit Perl, PHP beziehungsweise Ruby on Rails. Zur Datenspeicherung kommt entweder eine relationale Datenbank oder das Dateisystem zum Einsatz. Manche Blog-Software besitzt Funktionen, die weitere Software verlangen; beispielsweise für die Grafikverarbeitung Bibliotheken wie GD oder ImageMagick. Des Weiteren erlauben einige Produkte eine Erweiterung ihrer Funktionen mit Plug-ins.

Nach diesen grundlegenden Systemeigenschaften sind die eigentlichen Blog-Funktionen an der Reihe. Verlangt der Einsatzzweck nach mehreren oder gar beliebig vielen Blogs oder genügt es, wenn die Software eins oder eine begrenzte Zahl zulässt? Genauso stellt sich die Frage nach der Anzahl der Autoren. Insbesondere im Firmenkontext ist die Rechtevergabe ein zentraler Punkt. Erlaubt das System die Zuweisung von Rollen an Benutzer (Administrator, Redakteur, Autor et cetera)? Was ist mit der Kommentarfunktion? Lässt es sich steuern, ob Kommentare überhaupt, nur anonym oder nur angemeldet erlaubt sind? Um Artikel in einem Blog zu finden, ist eine Kategorisierung über Schlagworte (Tags) üblich. Eine eingebaute Suchfunktion kann darüber hinaus nicht schaden. Für die Autoren sind ein WYSIWYG-Editor und die Speicherung als Entwurf sinnvoll.

Für ein eigenes grafisches Design gibt es verschiedene Ansätze, etwa einen Template-Mechanismus, eventuell inklusive Template-Editor, oder eine Formatierung über CSS. Einige Systeme bieten Skins an, umschaltbare Designvorlagen, die eine Änderung der Darstellung mit wenigen Mausklicks gestatten. Wünschenswert ist es außerdem, dass die Software die eigene Sprache unterstützt. Während die Verwaltung mehrsprachiger Blog-Artikel aufgrund des Übersetzungsaufwands vermutlich nicht ganz oben auf der Wunschliste steht, möchte man bei generierten Texten, wie Navigationselementen, die Wahl der Sprache haben.

## Korrektheit und Syndikation

Bei den Ausgabeformaten ist HTML nicht erwähnenswert, fraglich aber, ob es sich um standardkonformes HTML oder XHTML handelt. Ebenso ist ein Syndikationsformat (RSS, Atom) zur automatisierten Weitergabe von Inhalten

**iX-TRACT**

- Wer sein Webtagebuch (Blog) nicht bei einem Dienstleister betreiben will, braucht Software – die ist erfreulicherweise kostenlos und einfach zu installieren.
- Die sieben hier vorgestellten, in verschiedenen Sprachen geschriebenen Blog-Pakete eignen sich teils für Gelegenheitsblogger, teils sind sie an der Grenze zum Content-Management-System angesiedelt.
- Manche Pakete sind auf einen einzigen Blog beschränkt, andere erlauben beliebig viele.

„state of the art“. Weniger häufig sind E-Mail-Benachrichtigungen anzutreffen, die beispielsweise den Eingang eines neuen Kommentars anzeigen.

Wenn es um die Handhabung von Bildern geht, die nicht nur verwaltet, benannt, geändert oder gelöscht, sondern darüber hinaus verarbeitet werden, verschwimmen die Grenzen zwischen Blog und Web Content Management.

Last, but not least, ist bei einem offenen System wie einem Blog das Augenmerk auf den Schutz zu richten. Neben der Benutzerverwaltung gehört zumindest bei einer (nach Registrierung) offenen Kommentarfunktion die Frage dazu, wie ein Administrator unerwünschte Kommentare (Spam) verhindern kann. Insbesondere wenn bekannte Systeme wie Wordpress, Movable Type oder Serendipity zum Einsatz kommen, sind die Schnittstellen für das Anfügen von Kommentaren bekannt und lassen sich von Spammern leicht ausnutzen.

Nach diesem kurzen Überblick über zu erwartende Eigenschaften und Funktionen von Blog-Systemen geht es nun in medias res. In der Tabelle sind Details zu allen betrachteten Systemen zu finden. Die Auswahl erfolgt nach den zentralen Kriterien:

– Es handelt sich um Open-Source-Software.
– Es handelt sich um installierbare Software, nicht um ein Blogging-Portal.
– Die Software macht einen „lebendigen“ Eindruck. Letzte Einträge im projekteigenen Blog aus dem Jahr 2003 sind ein Ausschlusskriterium.

Den letzten Punkt könnte man als unnötig ansehen, schließlich besteht die (zumindest theoretische) Chance, dass eine Software schon vor Jahren so gut war, dass eine Weiterentwicklung nicht erforderlich ist. Wenn es aber um Open Source geht, wofür es häufig keinen kommerziellen Support gibt, ist es beruhigend, eine aktive Community als Ansprechpartner bei Schwierigkeiten vorzufinden.

Für einige Systeme folgt nun eine vertiefende Beschreibung, die über die Auflistung in der Tabelle hinausgeht. Alle Produkte (und weitere) befinden sich auf der Heft-CD. Es geht los mit einem der wenigen in Java geschriebenen Produkte.



## Auf CD: 22 Blog-Systeme

Die sieben in diesem Artikel getesteten Softwarepakete geben zwar einen guten Überblick, aber natürlich existieren wesentlich mehr Werkzeuge dieser Art.

22 Blog-Systeme, darunter die im Artikel besprochenen, haben wir auf die Heft-CD zu dieser Ausgabe gepackt, nebst vier „Hilfsmitteln“, die das Installieren erleichtern. In der folgenden Aufstellung sind die letztgenannten zuerst aufgeführt, anschließend die Blogging-Pakete. Bei diesen ist in Klammern jeweils die Implementierungssprache vermerkt.

**XAMPP:** Apache, MySQL, PHP, Perl – ein Apache-Friends-Projekt.

**MySQL:** Die freie Variante des DBMS für Mac OS X, Windows und im Quellcode.

**PostgreSQL:** Das andere freie DBMS darf natürlich nicht fehlen.

**Apache Tomcat:** Der Servlet-Container mit integriertem Apache-Webserver.

**Roller:** Gruppengeeignet und passend für große und kleine Sites. (Java)

**b2evolution:** Neben vollem Feature-Set Schmankerln wie Fotomanagement. (PHP)

**Beta-Blogger:** Schlankes Softwarepaket, das out of the box funktioniert und viele Anpassungsmöglichkeiten bietet. (PHP)

**BLOG:CMS:** Gilt als das kompletteste Paket, mit Wiki, Fotogalerie und mehr. (PHP)

**Blojsom:** Umfangreich, Multiuser-fähig, setzt aber viel voraus (Tomcat). (Java)

**Drupal:** Ein CMS mit integriertem Blog-Bereich, skalierbar von der Hobby- bis zur Enterprise-Site. (PHP)

**ExpBlog:** Leicht anpassbar und schnell, so der Projektverantwortliche; unter anderem mit einer Plug-in-Schnittstelle. (PHP)

**Geeklog:** 2001 in die Public Domain gebrachte Software mit differenziertem Sicherheitsmodell. (PHP)

**Greymatter:** Ein schlankes Blog-System, schnell durchschaubar. (Perl)

**Jlog:** Einfache, schlanke, schnelle Weblog-Software von Jeena Paradies. (PHP)

**Lifetype:** Mit Unterstützung für mehrere Blogs beziehungsweise Benutzer in einer Installation. (PHP)

**Mephisto:** In Rails entwickelt, mit einfachen CMS-Features. (Ruby)

**Movable Type:** Freie Weblog-Software zum Selbstinstallieren, vom kalifornischen Blog-Vermarkter Six Apart. (Perl)

**Nucleus:** CMS mit dem Schwerpunkt Weblog, die „Mutter“ von Blog:CMS. (PHP)

**Pivot:** Ein einfaches System, das außer PHP nichts Vorinstalliertes braucht. (PHP)

**Project Steve Guttenberg:** Weiteres einfaches System, das außer PHP nichts Vorinstalliertes braucht. (PHP)

**Serendipity:** Ein System, das 40 Plug-ins zur Erweiterung dabeihat. (PHP)

**SPIP:** Ein System, das besonders die Entwicklung mehrsprachiger Weblogs unterstützt. (PHP)

**Subtext:** Zeichnet sich nach Aussage der Macher durch gute Benutzbarkeit, Eleganz und Einfachheit aus. (.Net/Javascript)

**Textpattern:** Ein System, das Auszeichnungen mit Textile beherrscht und XHTML „versteht“. (PHP)

**toendaCMS:** Wie der Name andeutet – ein einfaches CMS, das auch Weblogs „kann“. (PHP)

**WordPress:** Wahrscheinlich das meistverbreitete Weblog-System, sowohl in einer selbst zu installierenden als auch in einer gehosteten Version existent. (PHP)



## Apache Roller

Ursprünglich hat Dave Johnson Roller als Beispielapplikation für einen Artikel (siehe [a] in den „Onlinequellen“) über Open-Source-Java-Entwicklungswerkzeuge geschrieben, und seit 2007 vertreibt ihn die Apache Software Foundation in der Version 4.0 unter ihrer Lizenz.

Roller ist eine in Java entwickelte Webanwendung mit Datenbankanbindung. Für den Betrieb setzt das Werkzeug einen Servlet-Container und eine Datenbank voraus. Am besten unterstützt sind Tomcat als Servlet-Container und die Datenbank MySQL. Diese sollten installiert und ein wenig Erfahrung mit beiden Werkzeugen sollte vorhanden sein. Roller lässt sich allerdings auch in anderen Konstellationen betreiben.

Die Installation ist unkompliziert: Nach dem Herunterladen und Entpacken des Zip-Archivs kopiert man das unter *webapp* liegende *roller*-Verzeichnis in das *webapp*-Verzeichnis des Servlet-Containers. In MySQL muss man eine Datenbank für die Tabellen der Webapplikation erzeugen und für das Login einen Benutzer und eine Rechtevergabe anlegen. Im Klassenpfad des Containers muss sich die Datei *roller.custom.properties* mit den notwendigen Einträgen befinden.

Damit ist Roller startklar und zumindest lokal unter der Adresse localhost:8080/roller/ ausführbar. Die zuerst ausgelieferte Webseite fordert noch zum Anlegen der Datenbanktabellen auf. Im darauffolgenden Hauptmenü

lassen sich neue Benutzer und Blogs einrichten. Zudem kann man für alle Blogs einen Front-Page-Blog oder eine gemeinsame Einstiegsseite setzen.

Der zuerst registrierte Benutzer erhält automatisch Superuser-Status und die vollen Administratorrechte. Er kann alle Blogs verwalten, editieren, neue Benutzer registrieren und ist zudem für die Einstellungen zuständig.

Nach dem Anlegen eines Account kann man sein erstes Blog erstellen. Außer dem Namen, einer Beschreibung und einem „Handle“, der angehängt an die URL von Roller auf das eigene Blog verweist, lässt sich ein Theme aus einer Liste vorgefertigter Designs auswählen. Themes ermöglichen die optische Anpassung und Gestaltung des Blog. Grundlage für die Gestaltung von Themes sind HTML, CSS und Velocity als Template-Sprache. Der in Roller integrierte Template-Editor erlaubt die Anpassung und Erweiterung von Themes.

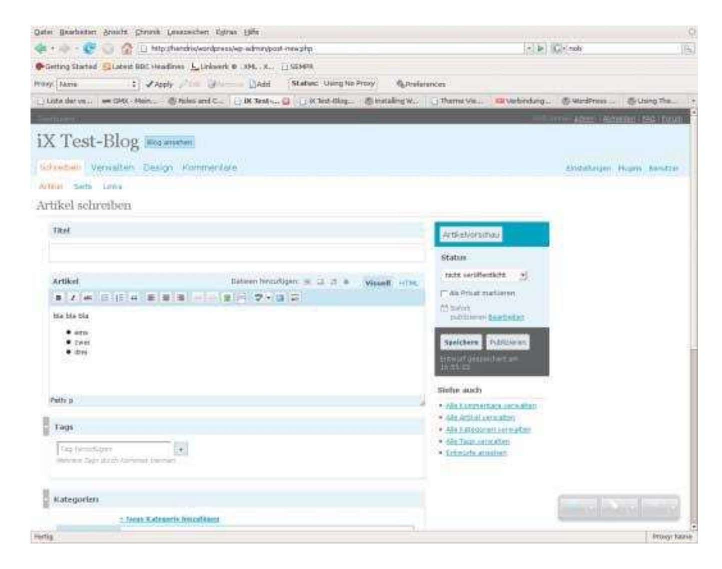
Inhaber eines Blog können weitere Einstellungen vornehmen. Dazu gehört die Auswahl eines Editors für das Verfassen von Einträgen. Zur Verfügung stehen ein einfacher Text- und ein WYSIWYG-Editor, der aber nicht in allen Browsern lauffähig sein soll (explizit genannt: Safari). Weitere Einstellungen betreffen die Anpassung des Blog an lokale Gegebenheiten, die Auswahl der zugelassenen Blog-Client-APIs, Spam-Prävention und Kommentare, die zugelassen, moderiert zugelassen oder nicht erlaubt sein können.

Zum Thema „Blog-Pings“ (siehe Glossar) bietet Roller vielfältige Einstellmöglichkeiten an. Es unterstützt dazu XML-RPC, wie ihn viele Seiten verwenden. Man kann die Registrierung bei einem Aggregator vornehmen und Ping-Targets festlegen und darüber hinaus automatische und manuelle Pings hinzufügen.

Wenn mehrere Personen an einem Blog arbeiten, spricht Roller von einem „Group Blog“. Ein solches entsteht durch Einladen anderer Benutzer. Die Rechtestufen „Admin“, „Author“ und „Limited“ erlauben unterschiedliche Berechtigungen der eingeladenen Personen.

Mit erweiterten Einstellungen kann der Verfasser unter anderem Einfluss auf die Anwendung von Plug-ins zur Gestaltung des Eintrags nehmen und die Erstellung von Kommentaren zeitlich begrenzen.

Im Administrationsbereich kann ein Benutzer Blogrolls (siehe Glossar) zusammenstellen und hochgeladene Da-




**Artikelerfassung in Wordpress: Außer der WYSIWYG-Ansicht können Autoren sich auch den HTML-Quelltext zeigen lassen (Abb. 1).**

teien verwalten. Dateien lassen sich in Ordner einsortieren und in Templates, Blog-Einträgen und Podcasts verlinken.

Seit Version 4.0 unterstützt Roller Podcasting (siehe Glossar). Damit können Autoren Dateien über den Blog-Newsfeed verteilen. Ein Podcast verhält sich wie ein Anhang an einen Blog-Eintrag.

Newsfeeds unterstützt Roller in den Formaten RSS 2.0 and Atom 1.0. Für jede Kategorie und für die Kommentare eines jeden Eintrags steht jeweils ein eigener Newsfeed zur Verfügung. Möglich ist außerdem der Im- und Export von Bookmarks und RSS-Listen im OPML-Format (Outline Processor Markup Language).

Roller unterstützt ebenfalls die Verwendung von Blog-Clients, mit denen Autoren ihre Beiträge „remote“ verfassen können. Sie lassen sich über den oben erwähnten XML-RPC-Mechanismus an Roller übertragen. Der kennt die Standards „MetaWeblog API“ und das „Atom Publishing Protocol“.

Zwar ist die Benutzerführung gut durchdacht, aber ein wenig stört die nicht vollständige Anpassung ans Deutsche, was zu einem Gemisch aus Deutsch und Englisch in den Konfigurationsseiten führt. Roller bietet zudem ein vernünftiges Sicherheitskonzept und Rollenverteilung. Dies ermöglicht das Betreiben von Gruppen-Blogs.

Die Vielzahl der genannten Eigenschaften macht Roller zu einer vielfältig einsetzbaren Blog-Plattform. Noch zu nennen ist die Option, Trackbacks (siehe Glossar) zu setzen.

Aufgrund seiner offenen 3-Schichten-Architektur und der weitgehenden Verwendung von Open-Source-Komponenten verfügt Roller über viele Erweiterungsmöglichkeiten (Plug-ins, Scripting, Template Engines et cetera).

Schließlich: Die Dokumentation ist umfangreich und gut zu verwenden, allerdings nur auf Englisch verfügbar. Und die Referenzliste der das Tool einsetzenden Firmen ist durchaus eindrucksvoll und belegt die Einsatzfähigkeit von Roller in großem Maßstab.



## Wordpress

Wordpress ist einer der großen Namen der Blog-Produkte. Neben der unter wordpress.org erhältlichen Software gibt es das korrespondierende Blog-Portal unter wordpress.com. Dort kann jedermann sein eigenes Blog einrichten und nebenbei die Software ausprobieren, ohne sie selbst installieren zu müssen.

Wer einen PHP-fähigen Webserver (bevorzugt Apache) und eine relationale Datenbank (bevorzugt MySQL) besitzt, kann die Installation in wenigen Minuten erledigen. Der Aufwand beschränkt sich auf der Datenbankseite auf das Anlegen einer neuen Datenbank und eines neuen Users mit vollen Rechten. Trägt man Namen und Passwort von Datenbank und Benutzer in der Wordpress-Config-Datei ein und verschiebt alle PHP-Dateien in ein Verzeichnis des Webservers, ist das Blog startklar.

Jede Installation entspricht genau einem Blog. Es spricht nichts dagegen, weitere Datenbanken und gegebenenfalls Datenbankbenutzer einzurichten sowie die PHP-Dateien in weitere Verzeichnisse zu kopieren. Im eigentlichen Sinn unterstützt eine Wordpress-Installation aber nur ein Blog.

Für die Umstellung auf eine deutschsprachige Oberfläche genügt der Download der diesbezüglichen Sprachdatei und ein weiterer Eintrag in der Konfigurationsdatei. Die Anleitung weist darauf hin, dass es nicht vollständig an verschiedene Sprachen angepasste „Themes“ gibt. Die Auswahl an solchen Themes ist groß. Derzeit sind auf themes.wordpress.net circa 1200 Gestaltungen zu finden, unterschiedlich nach Farben, Anzahl der Spalten, festem oder starrem Layout.

Wordpress unterscheidet die Rechte eines Benutzers nach dessen Rolle. Die Software kennt die fünf verschiedenen Rollen Administrator, Editor, Author, Contributor, Subscriber, deren Rechte die Dokumentation wie folgt beschreibt: Der Administrator hat vollen Zugriff, der Redakteur kann eigene Artikel veröffentlichen sowie eigene und fremde Artikel verwalten. Dagegen kann ein Autor nur eigene Artikel veröffentlichen und verwalten, ein Zuträger (Contributor) kann Artikel schreiben und verwalten, aber nicht veröffentlichen. Der Subscriber schließlich kann nur Kommentare lesen und Newsletter empfangen.

Artikel zu verfassen läuft über einen browserbasierten WYSIWYG-Editor, der es erlaubt, zwischen formatierter Ansicht und HTML-Quellcode umzuschalten. Darüber hinaus gibt es für Editoren Plug-ins, die das lokale Editieren und Veröffentlichen in einem Wordpress-Blog erlauben (siehe Abbildung 1).

Eine weitere Variante, Artikel in einem WP-Blog zu veröffentlichen, läuft über E-Mail. Die Software lässt sich unter Angabe eines POP-Hosts und -Kontos konfigurieren, sodass sie unter der konfigurierten Adresse eingehende Mails automatisch veröffentlicht. Die Betreffzeile wird dabei zum Titel und der Nachrichtentext zum Rumpf des Postings. Wordpress sortiert das Posting in der Default-Kategorie ein, und als Autor erscheint der Site-Admin. Außer einer Sortierung in Kategorien kann ein Autor Tags vergeben.

News-Feeds unterstützt Wordpress in den Formaten RSS 1.0 (die RDF-Fassung), RSS 2.0 und Atom. Leser, die einen Artikel als Lesezeichen anlegen möchten, sehen ansprechende Permalinks. Für die „Inter-Blog-Communication“ stehen die Funktionen Trackback und Pingback zur Verfügung.

Neue Kommentare lassen sich moderieren. Dabei besteht die Wahlmöglichkeit, alle eingehenden Kommentare zu moderieren, nur solche mit ausgewählten Schlagwörtern, die von bestimmten IP-Adressen stammen, oder solche, die eine definierte Anzahl Links enthalten.

## Movable Type

Auch Movable Type gehört zu den bekannten Vertretern seiner Zunft. Im Gegensatz zu Wordpress ist Movable

Type in Perl implementiert. PHP kommt nur optional zum Einsatz und zwar, wenn Seiten dynamisch veröffentlicht werden sollen. In den Werkseinstellungen führt die Software einige Änderungen wie das Löschen von Artikeln nicht sofort aus. Stattdessen ist das explizite „Veröffentlichen“ erforderlich. Dabei baut Movable Type alle Seiten neu auf, die anschließend als statische Dateien auf der Platte liegen. Die Vor- und Nachteile liegen auf der Hand: Statische Seiten senken die Rechenlast auf dem Server, erfordern aber die explizite Neugenerierung.

Die Software selbst wird nur einmal pro Webserver installiert. Die Ausführung erfolgt über CGI. Etwaigen Vorbehalten bezüglich der Performance der CGI-Ausführung (beispielsweise Aufwand für Prozessinitialisierung der CGI-Programme) steht das Argument gegenüber, dass CGI nur bei der administrativen und verfassenden Tätigkeit zum Einsatz kommt. Bei einer hohen Besucherfrequenz wird vor allem lesend auf das Blog zugegriffen, was aufgrund der statischen oder per PHP ausgelieferten Seiten keinen CGI-Overhead erfordert.

Eine Installation kann beliebig viele Blogs erzeugen. Deren statische Seiten liegen in der Regel unterhalb des Dokumentenwurzelverzeichnisses in je einem Verzeichnis. Wer mehrere Blogs betreiben möchte, hat nach der einmaligen Installation einen geringeren Aufwand als bei Wordpress. Außer der Software ist das Datenbankschema ebenfalls nur einmal anzulegen.

Schon beim Einrichten eines Admin-Account kann man auf eine deutsche Oberfläche umschalten. Das funktioniert weitgehend reibungslos, wenn man sich durch Sätze wie „Ihr letzter Eintrag war 2 minutes ago“ nicht aus der Bahn werfen lässt. Die Umstellung gilt für die Benutzeroberfläche des Account. Im Gegensatz dazu ist die Umstellung der Sprache für generierten Text im veröffentlichten Blog nicht so einfach. Weder die Suche in der Admin-Oberfläche, in der Dokumentation noch eine (allerdings kurze) Suchmaschinen-Recherche lieferten eine Antwort. Selbstverständlich funktioniert immer der Weg, die für die Seitengenerierung verantwortlichen Templates zu übersetzen. Dort sind Begriffe in englischer Sprache fest eingetragen (beispielsweise „Archives“ statt „Archive“). Ein Kommentar in einem Forum bezeichnet den Weg der eigenständigen Übersetzung als den zu gehenden Weg. Erstaunlich, dass es keine (leicht zu findenden) deutschen Templates gibt.

Für das Schreiben eines Blog-Eintrags steht der übliche WYSIWYG-Editor zur Verfügung. Des Weiteren gibt es drei alternative Eingabemethoden, bei denen gewisse Eingabezeichen in HTML-Auszeichnungen oder -Entities gewandelt werden. Es handelt sich um „Markdown“, „Smarty Pants“ und „Textile“; Details sind den „Onlinequellen“ zu entnehmen.

Einen fertigen Eintrag können Autoren als Entwurf speichern oder veröffentlichen, Letzteres auch unter Angabe eines in der Zukunft liegenden Veröffentlichungsdatums. Ein Eintrag besteht aus dem „Titel“, dem „Text“ und dem „erweiterten Text“. Letzterer ist auf Übersichtsseiten nicht sichtbar. Der „Text“ wird damit zur Einleitung des Artikels, und „Text“ und „erweiterter Text“ bilden gemeinsam den Rumpf des Blog-Eintrags.

Außer einem Blog-Eintrag kennt Movable Type „Seiten“. Sie werden genauso erstellt wie ein Eintrag, erscheinen aber nicht in der chronologischen Ordnung des Blog. Während die Adresse eines Eintrags dem Aufbau

```
http://hostname/blogname/jahr/monat/
eintragtitel.html
```

folgt, lautet die Adresse einer Seite

```
http://hostname/blogname/seitentitel.html
```

Dieses rudimentäre Content-Management-Feature erlaubt die Veröffentlichung von Webseiten im selben Look & Feel wie die der Blog-Einträge.



## Serendipity

Das PHP-basierte Serendipity ist laut eigener Aussage in der Standardausführung für den Gelegenheitsblogger ausgelegt. Bei einem Blick auf die Liste der Eigenschaften scheint das ein wenig untertrieben. Dazu später mehr. Serendipity liegt derzeit in der Version 1.3.1 vor. Die Installation setzt einen Webserver mit PHP-Support voraus. Am besten eignet sich laut Hersteller der Apache-Webserver. PHP muss mindestens in der Version 4.3.0 vorliegen,

die Entwickler empfehlen PHP 5.0. Serendipity unterstützt MySQL, PostgreSQL und SQLite.

Nach dem ersten Start bekommt man eine Systemdiagnose-Seite, der man den aktuellen Status der Anforderungen entnehmen kann. Zur Installation hat der Benutzer die Auswahl zwischen einer einfachen und einer fortgeschrittenen. Die einfache legt neben der Datenbankanbindung (Datenbank und der Benutzer müssen schon existieren) den Administrator, den Blog-Titel und eine Beschreibung fest. Eine Installation von Serendipity entspricht somit einem Blog. Weitere Einstellungen betreffen die Sprache und die Verwendung eines WYSIWYG-Editors. Experimentell können mehrere Blogs auf einer Installation von Serendipity aufsetzen. Dazu muss man allerdings Änderungen an der Konfigurationsdatei des Apache-Webservers vornehmen.

Serendipity ist nach der Installation sofort einsatzfähig. Nach einem Login gelangt der Autor auf eine „Verwaltungsoberfläche“, auf der er sämtliche Einstellungen vornehmen und Einträge bearbeiten kann.

In den eigenen Einstellungen kann der angemeldete Benutzer sein Passwort und Einstellungen zur Person ändern. Die Sprache des Blog und der Benutzeroberfläche lässt sich dort ebenso anpassen wie Voreinstellungen für Kommentare, Trackbacks und den zu verwendenden Editor.

Möchte man in seinen Einträgen Kategorien verwenden, muss man sie vor der Erfassung seines ersten Eintrags erstellen. Kategorien können frei gewählt und geschachtelt werden. Neue Einträge kann man in mehrere Kategorien einordnen.

Texterfassung läuft wie üblich in Feldern. Der Editor kann zwischen einem reinen Textmodus und einem WYSIWIG-Editor umgeschaltet werden. Ein Textfeld dient der Erfassung des Teasers, ein zweites der Erfassung des eigentlichen Textes. Jeder Eintrag erfordert die Angabe von Titel und Veröffentlichungsdatum. Das Datum kann in der Zukunft liegen. Weitere Einstellungen betreffen Kommentare und Trackbacks.

In einem Kommentarmanager kann ein Autor Kommentare je nach Berechtigung suchen, moderieren, bearbeiten, löschen und Antworten verfassen.

Veröffentlichte Einträge und Kommentare können Nutzer als RSS- und Atom-Feeds in allen bekannten Versionen abonnieren; RSS-Feeds auch pro Kategorie.

Autoren haben die Möglichkeit, das Aussehen und Verhalten von Serendipity über Styles und Plug-ins zu beeinflussen. In der Standardausführung stehen circa 20 Templates zur Auswahl. Einige verfügen über eine „Angepasste Admin Oberfläche“, mit der man erweiterte Einstellungen vornehmen kann.

Herzstück von Serendipity ist seine Erweiterungsmöglichkeit über Plugins. Das Paket unterscheidet zwei Arten: Seitenleisten-Plug-ins können links, rechts oder versteckt angeordnet werden. Dazu zählen beispielsweise die Plug-ins Kalender, Suche, Kategorien und Blog abonnieren. Ereignis-Plugins erweitern den Blog um zusätzliche Funktionen. Dazu zählen Textformatierung, Spam-Schutz, Browser-Kompatibilität, Hervorheben von Suchwörtern, Mailing von Artikeln, Statistiken, externer Blockroll-Feed und vieles mehr.

Schon in der Standardinstallation ist ein mächtiges Plug-in zum Spam-Schutz aktiv. Es bietet dem Autor IP-Sperrung, Wortfilter, grafische Captchas (siehe Glossar), automatische Aktivierung der Kommentarmoderation nach Alter des Textes und diverse Trackback/Pingback-Validierungsmethoden. Das Spartacus-Plug-in erlaubt es dem Benutzer darüber hinaus, weitere Templates und Plug-ins direkt aus dem Netz zu installieren.

Für ein Blog können mehrere Benutzer registriert werden. Serendipity unterscheidet die Rechte eines Benutzers nach seiner Zugehörigkeit zu einer oder mehreren Gruppen. Gruppenrechte sind frei konfigurierbar. Aus einer Liste von Rechten lassen sich für jede Gruppe die gewünschten auswählen.

Zur Verwaltung des Blog stellt Serendipity umfangreiche Einstellungen zur Verfügung. Diese sind unterteilt in die Blöcke Datenbankeinstellungen, Pfade, Permalinks, generelle Konfiguration, Design und Optionen sowie Bildkonvertierung. In den Einstellungen zu Design und Optionen lassen sich unter anderem Referrer-Tracking, URL-Rewriting und GZIP-Komprimierung einschalten.

Wer von einer anderen Blog-Software auf Serendipity umsteigen will, sollte im Import-Bereich für gängige Blog-Software (erfolgreich) suchen. Ein reiner RSS-Import/-Export wird ebenfalls angeboten.

Audio-, Video- und Bilddaten verwaltet eine Mediendatenbank. Benutzer können Medien hochladen und in geschachtelten Verzeichnissen speichern. Bilder lassen sich im Editor über eine Auswahlseite direkt einfügen.

Trackbacks erkennt Serendipity automatisch anhand von HTML-Links in den Einträgen und schickt sie an die entsprechende Seite. Außerdem kann man Trackbacks über ein Plug-in manuell verschicken. Pingbacks verwaltet das „Weblog ping Event plugin“. Sie werden bei der Veröffentlichung des Eintrags an die entsprechenden Seiten gesendet.

Der Plug-in-Mechanismus und die umfangreiche Auswahl an zur Verfügung stehenden Plug-ins machen die Software nicht nur für Gelegenheitsblogger interessant. Umfangreiche Konfigurationsmöglichkeiten, mit denen sich Serendipity fein an die eigenen Bedürfnisse anpassen lässt, gefallen ebenso wie die einfache, aber effektive Benutzerverwaltung.

Editierfunktionen, Kommentarmanagement, Mediendatenbank und die funktionierende Sprachanpassung der Benutzeroberfläche runden das Bild ab.

## Textpattern

Ursprünglich hat Dean Allen Textpattern entwickelt. Er zeichnet auch für das oben genannte Textile verantwortlich. So überrascht es nicht, dass Textpattern einen wesentlichen Unterschied zu anderen Systemen aufweist: Es gibt keinen WYSIWYG-Editor. Stattdessen ist die standardmäßig aktivierte Eingabemethode die von Textile, das heißt eine proprietäre, an Mediawikis erinnernde Auszeichnungssyntax. Eine Vorschau zeigt wahlweise den resultierenden XHTML-Code oder die formatierte Ansicht. Einen Eindruck von der Eingabe vermitteln die Abbildungen 2 und 3.

Ansonsten gibt es viele Ähnlichkeiten mit schon vorgestellten Systemen. Textpattern basiert auf PHP und einem DBMS wie MySQL. Die Installation gestaltet sich genauso wie bei anderen Systemen, Angabe von Datenbank- und Benutzername genügen. Bei eventuell auftretenden Fehlermeldungen darf man ruhig kreativ sein. So beschwert sich Textpattern über eine nicht vorhandene Datenbank, obwohl die wahre Fehlerursache fehlende Rechte des Datenbank-Benutzers sind.

Der erste Eindruck ist positiv. Das System wirkt nicht überladen sondern aufgeräumt. Allerdings ist es nicht so anwenderfreundlich wie andere. Das zeigt sich an den Zielgruppen, die die Webseite zum Textpattern-Buch (text patternsolutions.com) nennt:

## Auswahl kostenlos erhältlicher Blogging-Software

| Programm | Apache Roller | Wordpress | Mephisto | Movable Type | Textpattern |
|---|---|---|---|---|---|
| Website | roller.apache.org | wordpress.org | mephistoblog.com | www.movabletype.org | textpattern.com |
| aktuelle Version | 4.0 | 2.5.1 | 0.8, „Drax“ | 4.15 | 4.0.6 |
| letzte Aktualisierung | 12.07 | k. A. | 18.04.08 | 24.01.08 | k. A. |
| Lizenz | Apache Software License | GPL | Mephisto license | GPL2/Commercial | GPL |
| mehrsprachige Bedienung | ja | ja | ja | ja | ja |
| **Technik** | | | | | |
| minimale Voraussetzungen | Java 1.4 Servlet 2.3/JSP 1.2-Appl.server, am besten Tomcat, MySQL | Webserver, PHP 4.3, MySQL 4.0 | Apache, Ruby on Rails 1.2.3, Datenbank | Webserver, Perl, Datenbank (MySQL, PostgreSQL, SQLite), optional: Mailserver, PHP | Webserver, PHP 4.3, PHP, MySQL 3.23 |
| Datenspeicher | Datenbank | Datenbank | Datenbank | Datenbank | Datenbank |
| **Funktionen** | | | | | |
| Anzahl Blogs | unbegrenzt | 1 | 1 | unbegrenzt | 1/unbegrenzt über DB-Präfix |
| Anzahl Autoren | unbegrenzt | unbegrenzt | unbegrenzt | unbegrenzt | unbegrenzt |
| Kommentare | ja | ja | ja | ja | ja |
| Blogroll/Linkroll | ja | ja | ja | ja | ja (Link-Management) |
| Aggregatoren | ja | ja | nein | nein | nein |
| Suche | ja | ja | ja | ja | ja |
| Kategorien | ja, pro Blog | ja | ja | ja | ja |
| Tags | ja | ja | ja | ja | nein |
| URL-Rewrite | nein | ja | ja, über Konfigurationsdatei | ja | ja |
| Trackbacks/Pingbacks | ja | ja | nein | ja | ja |
| Blog via E-Mail | nein | ja | nein | nein | nein |
| unterstützte Standards | W3C-Standards | W3C-Standards | W3C-Standards | XHTML, CSS | XHTML, CSS |
| Forum | nein | nein | nein | nein | nein |
| Umfragen | nein | nein | nein | nein | nein |
| Statistiken | nein | ja | nein | ja | nein |
| **Editierfunktionen** | | | | | |
| WYSIWYG-Editor | ja | ja | nein | ja | nein |
| Draft/Preview Modus | ja | ja | ja | ja | ja |
| Revisionen | nein | nein | ja | nein | nein |
| Moderation von Einträgen | ja | ja | nein | ja | ja |
| **Gestaltung** | | | | | |
| Skins/Themes/Styles/Templates | ja | ja | ja | ja | CSS |
| Template-Editor | ja | nein | ja | ja | ja |
| Smileys | ja | ja | nein | ja, Plug-in | nein |
| Benutzerprofile | nein | ja | nein | ja | k. A. |
| **Ausgabeformat** | | | | | |
| Syndication Formate (RSS, Atom) | RSS 2.0, Atom 1.0 für Einträge und Kommentare | RSS 1.0, 2.0, Atom | Atom | Atom | RSS, Atom |
| E-Mail-Benachrichtigung | ja | ja | nein | ja | ja |
| PDF-Ausgabe von Einträgen | nein | nein | nein | ja | nein |
| **Medien** | | | | | |
| Medien-Upload | ja | ja | ja | ja | ja |
| Medienmanager | ja | ja | ja | ja | nein |
| Podcasting | ja | ja | nein | ja, Plug-in | nein |
| Komprimierung (GZIP) | nein | ja | nein | nein | nein |
| **Schutz** | | | | | |
| Registrierung neuer Benutzer (öffentliche Registrierung) | ja | ja | nein | ja | nein |
| Benutzerverwaltung | ja | ja | ja | ja | ja |
| Benutzergruppen/Rechte-verwaltung | Editor, Author and Limited | Administrator, Editor, Author, Contributor, Subscriber | nein | ja | ja |
| Antispam (Wortfilter, IP-Sperrung) | ja | ja | ja | ja | nein |
| Kommentarmanager | ja | ja | ja | ja | nein |
| **Sonstiges** | | | | | |
| Import/Export | nein | ja/ja (WordPress Extended RSS) | nein | ja/ja | nein |
| Plug-ins | ja | ja | ja | ja | ja |
| unterstützte APIs | Blogger, MetaWeblog, Atom Publishing Protocol | Blogger, Moveable Type, MetaWeblog | MetaWeblog API | MetaWeblog | Blogger, MetaWeblog |
| Support | Projekt-FAQ, -Wiki, Mailingliste, Bugtracking | FAQ, Forum | FAQ, Wiki, Forum | Community-Foren | Forum |
| Dokumentation | User-, Installation-, Template-Guide | Getting started, Working with Wordpress, Design and Layout, Advanced Topics | Setup-, User-Guide, teilweise nicht erreichbar | Installation-, Authors-, Designer-, Developer-Guide | Wiki, TextBook (user manual) |
| Referenzen | Sun, IBM, JRoller.com | wordpress.com | prototypejs.org/blog | radar.oreilly.com | s. welovetxp.com |

| Drupal | Serendipity |
|---|---|
| drupal.org | www.s9y.org |
| 6.2 | 1.3.1 |
| 09.04.08 | 22.04.08 |
| GPL (Core), andere (Module) | BSD |
| ja | ja |
| | |
| Webserver, PHP 4.1, MySQL 4.3, PostgreSQL 7.4 | Webserver, PHP, MySQL, PostgreSQL, ImageMagick |
| Datenbank | Datenbank |
| | |
| 1 | 1, mehrere via shared library (experimentell) |
| unbegrenzt | unbegrenzt |
| ja, Core-Plug-in | ja |
| ja, Core-Plug-in | ja |
| ja, Core-Plug-in | ja |
| ja, Core-Plug-in | ja |
| ja | ja, Unterkategorien möglich |
| ja, Taxonomien | nein |
| ja, Core-Plug-in | ja |
| ja, Core-Plug-in | ja |
| nein | nein |
| XHTML, CSS | W3C-Standards |
| ja, Core-Plug-in | nein |
| ja, Core-Plug-in | nein |
| ja, Core-Plug-in | ja |
| | |
| Standard nein, Plug-ins ja | ja |
| ja | ja |
| ja | nein |
| nein | nein |
| | |
| ja | ja |
| ja, Plug-in | ja, soweit einzelne Templates das unterstützen |
| nein | ja |
| ja | nein |
| | |
| RSS 2.0 | RSS, Atom |
| ja | ja |
| nein | nein |
| | |
| ja | ja |
| nein | ja |
| nein | nein |
| ja | ja |
| | |
| ja, moderiert, E-Mail-Verifikation | ja |
| ja | ja |
| ja, anonym and authentifiziert, Gruppen sind erweiterbar, Access/Deny-Profile (User, E-Mail, Host) | ja, frei konfigurierbar |
| ja | ja |
| ja | ja |
| | |
| Plug-in, nicht 6.x | ja/ja |
| ja, installierbar | ja |
| Blogger, MetaWeblog, Moveable Type (nicht ganz vollständig) | Blogger, Moveable Type Extension to Blogger |
| Foren, Mailinglisten, Gruppen-Website | k. A. |
| Getting Started, Beyond the Basics, Theming-Guides | Installation, User, Technical |
| Yahoo! Research, MTV UK, Warner Brothers, Sony BMG | s. www.s9y.org/18.html |

– Webdesigner, die XHTML und CSS beherrschen, sich aber nicht mit serverseitiger Programmierung und Datenbanken beschäftigen möchten.

– PHP-Entwickler, die ein CMS suchen, auf dem sie eigene Funktionen aufsetzen können.

An mehreren Stellen heißt es ausdrücklich, dass Textpattern ein CMS sei, nicht nur ein Blog-System. Da dies auch für andere Produkte gilt, ist zumindest festzustellen, dass die Grenzen zwischen Blog und CMS fließend sind. Textpattern kennt das Konzept von „Sections“, denen geschriebene Seiten zugeordnet werden können. Darüber hinaus ist es nicht auf den ersten Blick als CMS zu erkennen; es sei denn, man versteht das Verwalten, Herausgeben, Veröffentlichen eines Weblog als eine Content-Management-Tätigkeit.

Die Dokumentation lässt zu wünschen übrig. Es gibt zwar ein Wiki, das Informationen in mehreren Sprachen enthält, aber die deutschen Texte scheinen unvollständige Übersetzungen der englischen Seiten zu sein, was einen frühen Wechsel auf die Originale nahelegt. Selbst hier bleiben allerdings Fragen offen.

Von Haus aus bietet Textpattern eine Admin-Oberfläche in mehreren Sprachen, aber keine Sprachauswahl für das veröffentlichte Blog. Zu diesem Zweck steht ein Plug-in zur Verfügung. Wie bei anderen Produkten sind bei Textpattern die Plug-ins wichtig. Unter den Entwicklern und Patch-Zuträgern kam es im vergangenen Jahr zu Bewegung. Eine Gruppe von Programmierern war nicht zufrieden mit der Richtung, die die Entwicklung von Textpattern nimmt. Sie wollten einen „Community branch“ im Subversion-Repository, in dem sie neue Features implementieren könnten. Nach den heute noch zugänglichen Forumsdiskussionen wollten die Kernentwickler von Textpattern diesem Schritt nicht zustimmen.

Als Ergebnis gibt es seit einigen Monaten unter dem Namen xPattern (xpattern.net) einen Ableger des Projekts. Als Ziel ist auf der Webseite zu lesen: „It’s (sic!) goal is to improve the application to better fit the needs and desires of the community at large.“ Zurzeit steht noch kein Paket zum Download bereit. Welche Auswirkungen diese Bewegung auf Textpattern hat, lässt sich von außen kaum voraussehen. Zahlenmäßig scheint das „Team xPattern“ durchaus Gewicht zu haben. Die Webseite nennt 20 „aktive Mitglieder“, während Textpattern drei „Kernentwickler“ und eine Reihe von „Forummoderatoren und Enthusiasten“ aufführt. Zumindest solange xPattern keine Release zu bieten hat, ist die Frage nach der richtigen Textpattern-Distribution einfach zu beantworten: Es gibt nur eine.



## Drupal

Drupal ist ein weiterer Vertreter der in PHP realisierten Blog-Systeme. Die Software liegt mittlerweile in der Version 6.2 vor und bietet gegenüber der Vorgängerversion 5.x einige Neuerungen. Details zu den Neuerungen sind in der Mai-*iX* zu finden [1].

Die Installation verläuft nach bekanntem Muster. Anlegen einer Datenbank und eines Benutzers mit den notwendigen Zugriffsrechten, entpacktes Paket in ein Webserver-Verzeichnis verschieben und Starten im Browser. Drupal stellt keine großen Anforderungen an das System: einen Webserver, der PHP 5.x unterstützt, und MySQL 4.3 beziehungsweise PostgreSQL 7.4 oder neuere Versionen.

In der Folge arbeitet man Schritt für Schritt folgende Punkte ab: Auswahl der Sprache (Deutsch noch nicht für Version 6.x), Überprüfung der Anforderungen, Datenbankkonfiguration samt Anlegen der Tabelleninstallation, Konfiguration des Site-Namens, des Administratorenkontos, Zeitzone et cetera.

Nach Fertigstellung bekommt der Installateur eventuelle Fehlermeldungen mitgeteilt. Keine Verbindung zum E-Mail-Server oder ein nicht laufender Cron sind als typisch zu nennen. Cron ist unverzichtbar, da Drupal ihn für zeitgesteuerte Aufgaben verwendet.

Auf der Einstiegsseite findet sich neben dem Login eine Fortsetzung des Setup. Der wichtigste Punkt ist „Enable additional functionality“. Dort kann man viele Funktionen einschalten, die in der Default-Installation nicht eingerichtet sind. So sucht man zunächst vergeblich die Blog-Funktion. Weitere zuschaltbare Module betreffen Pings und Trigger, mit denen sich Aktionen zu Events (beispielsweise „neuer Inhalt erzeugt“) verwalten lassen. Module zur Administration von Benutzerprofilen stehen ebenfalls zur Verfügung (Suche, Statistik, Filter und Taxonomy). Mit Letzterem kann der Administrator Tags und selbstdefinierte Ausdrücke zur Kategorisierung des Inhalts festlegen. Weitere Module stehen zum Download unter drupal.org/project/modules bereit.

Neben „Blog entries“ bietet Drupal die Content-Typen, „Book page“, „Story“, „Page“, „Poll“ und „Forum topic“. Diese kann der Administrator einzeln als Module zuschalten. Zusammen mit der für jeden Inhaltstyp verwendbaren Versionsverwaltung ist Drupal ein integriertes Content-Management-System, mit dem man außer Blogs normale Webseiten und Foren aufbauen kann.

Mit der umfangreichen Benutzer- und Rechteverwaltung verwaltet der Administrator neue Benutzer in jeder Hinsicht. Er kann eine Registrierung komplett verhindern, nur moderiert zulassen oder eine Registrierung via E-Mail erzwingen. Die Zugriffsrechte der Benutzer lassen sich funktions- und modulorientiert in Benutzerrollen gruppieren. Neben den Default-Gruppen „anonymous user“ und „authenticated user“ können beliebig viele Rollen verwaltet werden. Über „Access rules“ lässt sich der Zugang zum System steuern. Drupal erlaubt die Vergabe von Regeln für den Benutzernamen, die E-Mail-Adresse oder den Hostnamen (Allow, Deny). Zusätzlich steht das Modul OpenID dem Benutzer für die Anmeldung zur Verfügung. OpenID ermöglicht ein plattform- und anwendungsübergreifendes Identitätsmanagement.

Die Gestaltung eigener Webseiten findet in den Punkten „Blocks“, „Menus“, „Modules“ und „Themes“ statt. „Blocks“ sind „Kästen“, in denen Inhalte ausgegeben werden und die sich auf der Seite per Drag & Drop in Regionen anordnen lassen (Kopf, Fuß, Content oder den Sidebars). Module stellen solche neuen Blöcke bereit. Für das Design der Seiten stehen eine Reihe von Themes zur Auswahl, zusätzlich lassen sich weitere unter drupal.org/project/themes nachladen.

Neue Inhalte erstellen Autoren durch Auswahl eines „Content type“ und anschließende Erfassung des Inhalts wie üblich in einem Textfeld; WYSIWYG gibt es per Default nicht, kann aber als Modul nachinstalliert werden. Autoren trennen Teaser auf Knopfdruck vom Haupttext ab. Weitere Einstellungen betreffen die Revisions- und Kommentarverwaltung, Dateianhänge und „URL path settings“, mit denen der Autor seinem Artikel einen neuen relativen Pfadnamen geben kann. In den „Publishing options“ kann er festlegen, ob der Artikel sofort zu veröffentlichen und damit auf der Eingangsseite sichtbar ist.

Von weiteren Eigenschaften seien hier nur ein paar erwähnt. Drupal bietet eine Kommentarverwaltung, mit Reports lassen sich Seitenfehler aufspüren und ein Datei-Upload existiert ebenfalls. RSS-Feeds können zu jeder Kategorie und jedem Autor abonniert werden. Weitere Fähigkeiten sind der Tabelle zu entnehmen.

Durch die Vielzahl der Module lässt sich Drupal gut erweitern und den eigenen Bedürfnissen entsprechend anpassen. Leider können viele Plug-ins bisher noch nicht mit der Version 6 arbeiten. Die Benutzer- und Rechteverwaltung lässt keine Wünsche offen.

## Mephisto

Der Blog von prototypejs.org läuft auf der Basis von Mephisto. Da die Entwickler Prototype innerhalb des Ruby-on-Rails-Projekts entwickelt haben, verwundert es nicht, dass Mephisto eine Rails-Applikation ist.

Die Installation von Mephisto gestaltet sich etwas umfangreicher, wenn erst ein entsprechendes Rails-Environment geschaffen werden muss. Eine Installation von Mephisto entspricht einem Blog. Grundlage für die Begutachtung in diesem Artikel war der in Rails integrierte Webserver Webbrick. Die Datenbankanbindung an MySQL gestaltet sich mit einem *gem install mysql-ruby* und Editieren einer Konfigurationsdatei einfach. Zum Schluss: *gem install tzinfo* – und Mephisto ist mit dem Aufruf *ruby script/server –e production* am Start.

Nach einem Login mit einem vorgegebenem Benutzer und Passwort präsentiert sich Mephisto mit einer Übersichtsseite, auf der aktuelle und vergangene Aktionen aufgelistet werden. Über Tabs kann man neue Einträge und Sektionen (Kategorien) erstellen sowie Dateien hochladen. Blog-Sektionen können mehrere Einträge enthalten, Seiten-Sektionen dagegen nur einen Eintrag pro Seite. Weitere Tabs führen zu spezialisierten Seiten der genannten Aktionen, zusätzlich stehen eine Design- und Benutzerverwaltung zur Verfügung.

Letztere ist einfach gehalten. Der vorgegebene Benutzer ist automatisch Administrator des Blog. Er kann neue Benutzer registrieren und ihnen Administrationsrechte erteilen. Ohne sie können Benutzer keine generellen Einstellungen vornehmen. Das Login eines Autors ist sperrbar. Benutzergruppen kann Mephisto nicht verwalten.

Templates regeln die Gestaltung der Oberfläche. Als Template-Engine kommt Liquid zum Einsatz, ein speziell für Rails-Anwendungen entwickeltes

## Glossar

**Aggregatoren**: Sie werden durch Blogs mit Update-Notification-Pings (siehe Pings) darüber benachrichtigt, dass neue Einträge vorliegen. Aggregatoren aktualisieren in diesem Fall die bei ihnen registrierten Newsfeeds der entsprechenden Blogs und veröffentlichen die neuen Einträge in einer fortlaufenden Übersicht.

**Blogroll/Linkroll**: Liste favorisierter Blogs oder Webseiten, die bevorzugt in der Sidebar eines Blog zu sehen sind. Die Einträge in der Liste sind frei editierbar und werden als Bookmarks bezeichnet.

**Captchas**: Mittel zur Spam-Vermeidung in Blog-Kommentaren. Captchas erfordern vom Benutzer die Eingabe einer zufälligen Buchstabenfolge auf Basis einer generierten Grafik, damit ein Kommentar angenommen wird.

**Pings**: Fremde Seiten können mit Update-Notification-Pings (kurz Pings) darüber informiert werden, dass neue Einträge auf der eigenen Seite vorhanden sind. Die benachrichtigten Seiten können automatisch die zugehörigen Newsfeeds neu laden (siehe Aggregatoren).

**Podcast**: Serie von Medienbeiträgen (Audio/Video), die über einen Newsfeed automatisch bezogen werden können.

**Syndication**: Der Begriff bezeichnet üblicherweise den Austausch von Inhalten zwischen verschiedenen Websites beziehungsweise die Übernahme von fremden Einträgen. Im Blog-Umfeld beschreibt der Begriff die automatische Erzeugung von Zusammenfassungen neu erschienener Einträge oder Kommentare in Form von Newsfeeds als RSS oder Atom.

**Trackbacks/Pingbacks**: Funktion, mit der Informationen über das Referenzieren von Einträgen und Kommentaren über einen automatischen Benachrichtigungsdienst ausgetauscht werden können. Einige Blog-Systeme unterstützen nur eine manuelle Eingabe des Trackback-Links des Eintrages, auf den Bezug genommen wird. Andere bieten eine automatische Trackback-Erkennung an (Trackback Auto Discovery).

**XML-RPC**: Extensible Markup Language Remote Procedure Call ist eine Spezifikation zum Methodenaufruf in verteilten Systemen. Der Transport der Daten läuft über HTTP, die Aufrufe selbst sind in XML ausgezeichnet.




**Texteingabe bei Textpattern: Wiki-ähnliche „Textile"-Auszeichnungen statt WYSIWYG-Editing (Abb. 2)**

**Textpattern: Vorschau der Eingabe (Abb. 3)**

Plug-in. Templates werden zu Themes zusammengefasst. Sie lassen sich importieren und – wiederum über die einzelnen Templates – anpassen.

Generelle Einstellungen finden sich etwas versteckt in einer Linkleiste am oberen Rand. Als Spam-Abwehr sind Einstellungen zur Überwachung von Kommentaren vorgesehen. Die werden in der Voreinstellung automatisch veröffentlicht, Administratoren können sie nachträglich moderieren, löschen oder auf „unapproved" setzen. Mephisto kann in der jetzigen Version außerdem das Plug-in Akismet zur automatischen Überwachung von Kommentaren einsetzen, das erfordert allerdings die Eingabe eines API-Schlüssels (akismet.com).

Neue Einträge erfassen Autoren in einfachen Textfeldern (kein WYSIWYG) – entweder in reinem HTML oder mit den Format-Plug-ins „Textile", „Markdown" und „Smarty Pants" (siehe die „Onlinequellen"). Einträge lassen sich in einer oder mehreren Sektionen veröffentlichen oder als Entwurf speichern. Das Veröffentlichungsdatum lässt sich festlegen und kann in der Zukunft liegen. Einen Artikel können Autoren in einer Voransicht überprüfen. Mephisto speichert Einträge im Normalfall mit Revisionen. Der Autor hat zusätzlich die Option, darauf zu verzichten.

Beim Versuch, den ersten Eintrag abzuschließen, trat ein Encoding-Fehler auf. In der Mephisto Google Group findet man Hilfe zu diesem Stolperstein, allerdings muss man zur Fehlerbeseitigung eine Änderung am Quellcode vornehmen.

Mephisto verfügt über ein Asset-Management genanntes Medienmanagement, mit dem man Dateien laden und verwalten kann. Es ist allgemein über einen Tab auf der Übersichtsseite zugänglich und steht zusätzlich während des Erfassens eines Artikels zur Verfügung. Von dort kann der Autor eine geladene Datei per Drag & Drop in das Editor-Feld ziehen (im Editor landet nur der Pfad der Datei). Das Layout muss er von Hand mit entsprechendem Markup vornehmen.

Derzeit funktioniert das Hochladen von Dateien nicht richtig. Scheinbar existiert ein Timing-Problem, und ein Upload-Versuch endet mit einem Fehler. Zwar lassen sich Dateien durch mehrfaches schnelles Drücken des Upload-Buttons hochladen, aber das ist nicht besonders anwenderfreundlich.

Veröffentlichte Einträge sind als Atom-Feed abonnierbar, allerdings stehen in der normalen Installation keine Feeds für Sektionen bereit. Dafür kann der Autor die Übersichtsseite mit den aktuellen und vergangenen Änderungen als Feed abonnieren.

Mephisto stellt alle grundlegenden Blog-Funktionen zur Verfügung, kann vom Umfang der Funktionen aber nicht mit Roller oder Serendipity mithalten. Konzeptionell ist Mephisto ein System mit Potenzial, derzeit eignet es sich jedoch nicht für den Gelegenheitsblogger. Über Plug-ins und Änderungen in den Konfigurationsdateien lässt sich die Software leicht an die eigenen Bedürfnisse anpassen – gute Kenntnisse in Ruby und Rails vorausgesetzt.

Einige Bugs in der derzeitigen Version sind lästig und erschweren die Arbeit. Hilfe bekommt man über die Mephisto Google Group, die Dokumentation ist nicht gerade umfangreich.

## Onlinequellen

[a] Building an Open Source J2EE Weblogger, David Johnson, 17.4.2002
www.onjava.com/pub/a/onjava/2002/04/17/wblogosj2ee.html

[b] Markdown
daringfireball.net/projects/markdown/

[c] Smarty Pants
daringfireball.net/projects/smartypants/

[d] Textile
www.textism.com/tools/textile/

# Fazit

Roller, Wordpress, Movable Type, Serendipity und Drupal vermitteln einen ausgereiften und stabilen Eindruck. Textpattern und Mephisto sind ebenfalls dazuzuzählen, allerdings trüben einige Anlaufschwierigkeiten das Bild ein wenig.

Bei den PHP-basierten Systemen läuft die Installation stets nach dem gleichen Muster ab, was bedeutet, alle Systeme lassen sich gleichermaßen einfach installieren. Aber selbst die Installation und Inbetriebnahme von Roller ist einfach und setzt nur geringe Vorkenntnisse im Umgang mit Servlet-Containern und Datenbanken voraus. Gleiches gilt für das in Perl implementierte Movable Type. Der Aufwand für das auf Rails basierende Mephisto ist etwas höher, es sei denn, die erforderliche Laufzeitumgebung ist schon vorhanden.

Wordpress und Mephisto sind Systeme für genau ein Blog. Jedes weitere erfordert eine weitere Instanz der Software. Textpattern unterstützte ursprünglich ebenfalls nur ein Blog; mittlerweile kann man bei der initialen Konfiguration ein Datenbankpräfix angeben. Verschiedene Präfixe erlauben mehrere Blogs auf derselben Datenbank. Alle anderen Systeme sind von Hause aus für mehrere Blogs ausgelegt. (hb)

CHRISTOPH LEISEGANG UND STEFAN MINTERT

arbeiten unter anderem als Web-2.0-Entwickler bei Linkwerk.com.

## Literatur

[1] Markus Franz; Web-CMS; Gemeinsam ans Web; Drupal 6: Neue APIs und mehr Komfort; *iX* 5/2008, S. 62








Twitter: Blogging, Instant Messaging und SMS in einem

# Das Geschnatter

Klaas Wilhelm Bollhoefer, Jens-Christian Jensen

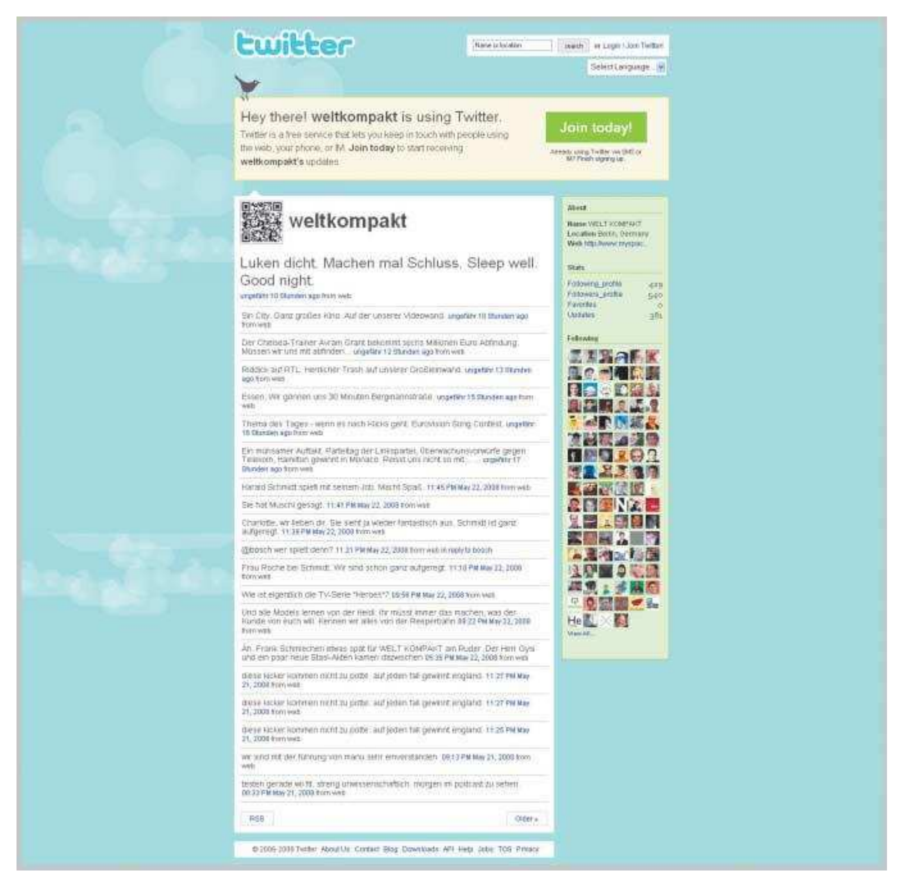
E-Mail war gestern, was die jüngste Internet-Generation betrifft. Die hält sich über Dienste wie Twitter auf dem Laufenden, das irgendwo zwischen Blogging und SMS als eine erfrischende Form der Kommunikation angesiedelt ist.

Oktober 2006: Schon wieder pulsiert ein neues Phänomen in der Blogosphäre. Technorati überschlägt sich innerhalb kurzer Zeit mit Sucheinträgen, viele staunen begeistert, andere hinterfragen den Sinn und beschwören den nächsten überschätzten 2.0-Hype-Service herauf. Die Rede ist von Twitter (engl. für Gezwitscher/Geschnatter), laut Wikipedia einem „Social networking“- und „Micro-blogging“-Dienst, in Wahrheit aber mehr als das. Twitter ist ein, wenn nicht der neue digitale Kommunikationsdienst der nächsten Jahre, „twittern“ (das nächste „googeln“ im Duden?) eine neue Form der Kommunikation, die langsam, aber sicher massentauglich werden könnte.

Twitter begann als Forschungs- und Entwicklungsprojekt der Firma Obvious, LLC in San Francisco im März 2006 und erblickte das Licht der virtuellen Welt im Oktober desselben Jahres. Seit April 2007 existiert Twitter, Inc. als eigenes Unternehmen. Das Programm ist in Ruby on Rails programmiert, eine offene API erlaubt das Integrieren von Twitter in beliebige Anwendungen. Seit April dieses Jahres ist Twitter in einer japanischen Version online und erlebt rasanten Zuwachs, was sicherlich der dort allgemein hohen Nutzung des mobilen Internet zu verdanken ist.

Wie viele Dienste der Web-2.0-Ära (Flickr, del.icio.us oder Youtube) beginnt Twitter mit einer einfachen Idee, und darin liegen der Reiz und die Stärke. Twitter stellt die einfache Frage „What are you doing?“ und stellt einen Dienst bereit, diese jederzeit und von jedem Ort schnell und einfach zu beantworten. Und das in maximal 140 Zeichen. Jede Antwort in Form einer Statusmeldung, Ortsbeschreibung, Frage, eines Gedankensplitters oder sonstigen Informationshäppchens (im Jargon „tweet“ genannt) wird je nach Voreinstellung in den Account-Daten an alle Twitterer oder den direkten Freundeskreis publiziert. Dafür muss man sich nur registrieren und erzeugt damit die eigene Twitterseite unter *twitter.com/Username*. Auf dieser Profilseite laufen alle publizierten Tweets chronologisch ein, einem Blog vergleichbar, werden archiviert, sind per Permalink adressier- oder per RSS-Feed syndizierbar. Andere bekannte Blog-Funktionen wie Kommentare oder Trackbacks sucht man vergeblich. Reduce to the max, um es mit der Smart-Werbung zu sagen.

Solche Seiten fungieren im Twitterversum zwar als zentrale Knotenpunkte, aber nur wenige Anwender dürften sie oft besuchen. Wie bei jeder Kommunikationslösung regiert bei Twitter das Prinzip der Dezentralität, im digitalen Zeitalter erweitert auf alle Kanäle. So kann man Tweets per (mobilem)




**So unterschiedlich diese Inhalte sind, durch das gegebene Format eines Tweet kann der Nutzer sie zu seinem persönlichen und individuellen Activity-Stream zusammenstellen (Abb. 1).**

Web-Interface, Browser-Plug-in, Instant Messenger (beispielsweise Jabber oder Google Talk), SMS, Mobile oder Desktop-Applikation (etwa der von vielen benutzten AIR-Application „twhirl“) schicken. Über dieselben Kanäle sind die Tweets anderer lesbar. Twitter unterscheidet dabei in „following“ und „followers“. Zu Ersteren zählen die Twitter-User, deren Beiträge Nutzer abonniert haben, bei Letzteren handelt es sich um diejenigen, die wiederum bestimmte Tweets abonnieren. Ein typischer Twitter-Client listet die Äußerungen derer, denen er folgt, ähnlich RSS-Readern chronologisch auf. Jeden Tweet kann man beantworten. Das Senden von Nachrichten ist möglich. Des Weiteren lassen sich einzelne Beiträge als Favoriten markieren.

Twitter ist kein Blogging, kein Instant Messaging, SMS oder Chat. Wo der Blog als digitales Tagebuch fungiert, asynchron aber (im Normalfall) von jedem kommentierbar, Instant Messaging und Chats die synchrone Eins-zu-eins- oder Many-to-many-Kommunikation in Echtzeit erlauben, nimmt Twitter von allem etwas und fügt es zu einer neuen Plattform für persönliche Kommunikation zusammen. So ist Twitter One-to-many, synchron und persistent. Hat man es einmal genutzt und sich darauf eingelassen, zieht einen diese neue Form des „Gesprächs“, des „Zuhörens“ und „Mitteilens“ in den Bann.

## Im Banne der persönlichen Plattform

Fluch und Segen zugleich scheint die bewusste Beschränkung eines Tweet auf 140 Zeichen zu sein, denn es setzt der Beschreibung dessen, was jemand mitteilen will, eine harte Grenze. Die Vorteile überwiegen jedoch klar und deutlich, und wer in die Welt von Twitter eintaucht, lernt das Reizvolle an den bewusst kurzen Statements enorm schätzen. Man ist gezwungen, kreativ mit der gegebenen Zeichenzahl umzugehen und vor allem nicht ausschweifend zu erzählen. Das Umfassende, teils Schwerfällige so mancher Blogposts ist nicht zugelassen – es geht um die kleinen Meldungen aus dem Alltag. Beim Lesen trudeln nach und nach die Tweets der Anwender ein, es entstehen kleine, lose verknüpfte Gespräche und man erhält ein wenig Einblick in das aktuelle Tun und Denken (für den Nutzer) wichtiger Personen. Es ist nicht Sinn und Zweck, alles zu verfolgen und zu lesen. Ist die Zeit da, schaut man rein, hört ein wenig zu, antwortet, nimmt selbst einen Eintrag vor. Um URLs mit möglichst geringer Zeichenzahl zu schicken, haben sich Alias-Dienste wie tinyurl.com, is.gd oder snurl.com bewährt.

Rund um Twitter hat sich wie zu erwarten ein unüberblickbares Dickicht aus Diensten entwickelt. So gibt es mit twitpic.com eine einfache Möglichkeit, Bilder (als URL) als Tweet zu posten, tweetalk.com erlaubt sogar das Versenden von Voice-Nachrichten, und sogenannte „hashtags“ (frei vergebene Tags) erlauben die Verschlagwortung eines Tweet, nach denen alle Anwender zentral unter hashtags.org suchen können. Mit tweetscan.com und summize.com gibt es zentrale Suchsites über alle öffentlichen Twitter-Posts. Darüber bietet twittervision.com den obligatorischen Geomapping-Service, twitterverse.com zeigt eine Tagcloud mit beliebten Begriffen und etliche andere Dienste, die hier bewusst und aufgrund offensichtlicher Platzbeschränkung nicht folgen sollen.

## Unternehmerisches Gezwitscher

Wo der eine nur seinen Freunden und Bekannten folgt, verfolgen andere Websites und Firmen. CNN twittert seine Schlagzeilen, Amazon.com das tägliche Sonderangebot. „Die Welt kompakt“ twittert live den Redaktionsalltag und diskutiert die morgige Ausgabe gerne mit dem Follower, während die amerikanischen Präsidentschaftskandidaten ihren Wahlkampfalltag verbreiten.

Das innovative Konzept von Twitter, gepaart mit der Kritik, dass Twitter zu simpel sei, hat eine Unzahl an Konkurrenten ins Leben gerufen. Bei Pownce.com kann der Nutzer eine Gruppenfunktion nutzen, um nur mit einem Teil seiner Freunde zu kommunizieren. Außer den normalen Nachrichten können Links, Dateien (inklusive Vorhaltung) und Veranstaltungen veröffentlicht werden. Jaiku.com verbindet Mikro-Blogging mit Aggregatsfunktionen. Ein Nutzer postet nicht nur Nachrichten, sondern kann außerdem automatisch externe RSS Feeds von Jaiku verschicken lassen. So lassen sich die eigenen Flickr-Fotos, ein Blog oder Tweets einbinden. Google sicherte sich das Know-

## Onlinequellen

| | |
|---|---|
| Twitter | www.twitter.com |
| Twitter mobil | m.twitter.com |
| Desktop Twitter Client, Adobe AIR | www.twhirl.org |
| Fotos per Twitter | www.twitpic.com |
| Voice-Nachrichten per Twitter | www.tweetalk.com |
| The most popular Twitter Apps | www.readwriteweb.com/archives/most_popular_twitter_apps_blogosphere.php |
| Twitter-Suche | summize.com |
| Twitter-Schlagwortsuche | hashtags.org |
| Twitter Googlemaps Mashup | twittervision.com/ |
| Twitter-API-Dokumentation | groups.google.com/group/twitter-development-talk |
| Tweet: Breaking News CNN | http://twitter.com/cnn |
| Tweet: Amazon Deals | http://twitter.com/amazondeals |
| Tweet: Welt kompakt | http://twitter.com/weltkompakt |
| Tweet: Barack Obama | http://twitter.com/BarackObama |

how der Entwicklerfirma im Oktober 2007, indem sie das finnische Unternehmen kaufte.

## Medien für den digitalen Prosumenten

Glaubt man der Blogosphäre, scheint Friendfeed derzeit der größte Konkurrent von Twitter zu sein. Friendfeed erlaubt es, von derzeit mehr als 30 Webservices Updates abzufragen und automatisch als Activity-Stream zu verschicken – sozusagen der „Lifestream“ des digitalen Prosumenten-Daseins. Zusätzlich können eigene Räume eingerichtet werden, in denen mehrere Teilnehmer in einen Stream Nachrichten schicken.

Trotz solcher Konkurrenten mit mehr Funktionen ist immer noch Twitter der König unter den Mikro-Blog-Diensten. Vielleicht ist es schlicht die Einfachheit, die Anwender so dankbar annehmen.

Mikro-Blogging lässt sich durchaus in der internen Unternehmenskommunikation einsetzen. Sind gängige Fragen wie „Wer will mittags mit zum kleinen Italiener?“ oder „Schaut euch mal die Website an“ nicht passende Fragen für ein asynchrones und dezentrales Medium? Der mobile Charakter lässt Applikationen wie Twitter noch attraktiver erscheinen, da Mitarbeiter außerhalb des Büros leicht informiert bleiben und sich selbst informieren können. Mikro-Blogging dürfte die offizielle E-Mail nicht ablösen, aber es ist eine erstzunehmende Alternative für den täglichen Kommunikationsfluss innerhalb von Projekten und Unternehmen.

## Fazit

Die jüngste Internet-Generation nutzt nicht mehr die E-Mail, sondern hauptsächlich Instant Messaging und soziale Netze für die Kommunikation. In diesen Trend passt das neue Prinzip des Mikro-Blogging, das sich seinen festen Platz in der zukünftigen Kommunikation im Netz sichern wird. Und die Verknüpfung von Mikro-Blogging und bestehenden Webdiensten ist absehbar, so haben Facebook und Xing schon diesbezügliche Funktionen in ihre Software integriert.

Mikro-Blogging, wie es Twitter etabliert hat, ist kein Hype, sondern „evolutioniert“ die Kommunikation im Internet und dürfte als Kommunikationsart in den kommenden Jahren fast unverzichtbar sein. (hb)


KLAAS WILHELM BOLLHOEFER

ist Director Beratung & Konzeption bei der Pixelpark AG in Berlin. Seine Spezialgebiete sind Enterprise 2.0, Immersive User Experiences, IPTV und Data Visualisation. Er twittert als *pixelklaas*.

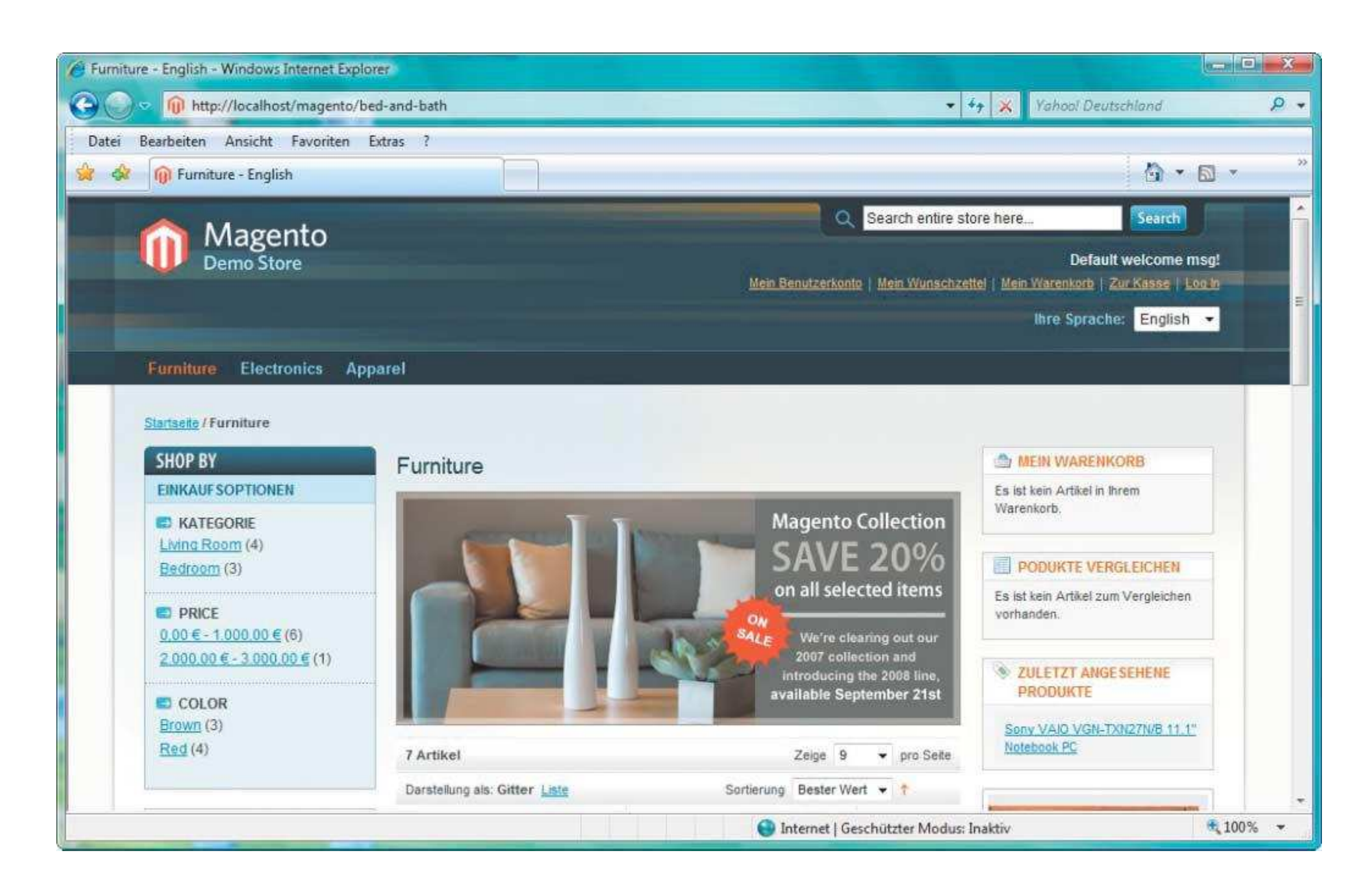
JENS-CHRISTIAN JENSEN

ist Senior-Berater bei der Pixelpark AG in Berlin. Seine Spezialgebiete sind der Einsatz von Informationstechnologie für interaktive und kollaborative Webdienste sowie soziale Netzwerke. Er twittert als *JcJensen*.










## Magento: Webshop auf Open-Source-Basis

# Kaufrausch

**Daniel Koch**

Systeme, mit denen man einen Onlineshop betreiben kann, gibt es reichlich. Aber entweder handelt es sich um teure kommerzielle Angebote, die Anwendung ist zu kompliziert oder es mangelt an Funktionen. Nichts von alledem trifft auf das neue Shop-System Magento zu.

Nach langer Alpha- und noch längerer Beta-Phase hat Version 1.0 des neuen Open-Source-Shop-Systems Magento das Licht der Welt erblickt. Nun stellt sich unweigerlich die Frage, was Magento bietet, was andere Shops nicht haben – oder was man bei anderen Lösungen erst (oft kostenpflichtig) nachrüsten muss. Da wäre zunächst die Multishop-Fähigkeit zu nennen, dank der man mehrere Shops unter einem Administrator-Account betreiben kann.

Besonders gelungen ist zudem das sogenannte One-Klick-Upgrade. Es erlaubt das Einspielen von Magento-Updates im Handumdrehen. Andere interessante Funktionen sind das Check-out, das auch den nicht angemeldeten Benutzer sämtliche Features benutzen lässt, die Suche mit Live-Vorschlägen, die Suchmaschinenoptimierung und die Mehrsprachigkeit. Und schließlich gibt es ein eingebautes CMS, über das der Shopbetreiber neue Seiten und Inhalte anlegen kann.

Neben diesen „Frontend-Funktionen“ hat Magento einiges für Entwickler zu bieten. So wurde der Shop ausschließlich in objektorientiertem PHP5-Code entwickelt und setzt vollständig auf das Zend-Framework. Mit Dataflow bietet die Software außerdem eine einheitliche Schnittstelle für Erweiterungen durch Dritte, die dafür sorgen dürfte, dass die Zahl zusätzlicher Funktionen rasch steigt.

## Magento installieren

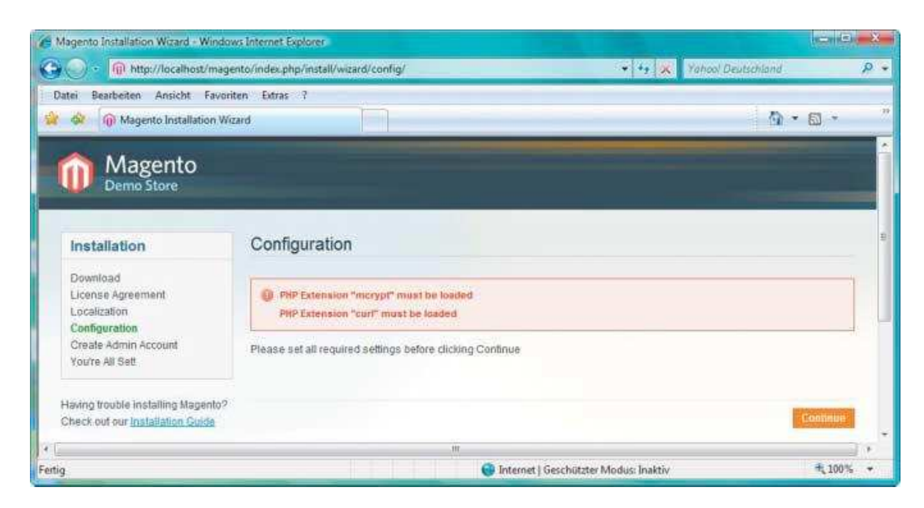
Als Systemvoraussetzungen benötigt Magento Apache 1 oder 2, PHP 5.2 (oder neuer), MySQL 4.1.2 (oder neuer) und einen Sendmail-kompatiblen Mail Transfer Agent. Zudem weisen die Entwickler ausdrücklich darauf hin, dass Magento derzeit nur unter Linux vollständig läuft. Allerdings funktioniert Magento auch fast fehlerfrei auf Windows-Systemen. Hier klappt aber der Upload von Produktbildern über das Backend nicht. Bleibt zu hoffen, dass die Magento-Entwickler hier schleunigst nachbessern.

Zur Installation muss das 30 MByte große Verzeichnis auf den Server geladen und dort aufgerufen werden. Magento arbeitet mit einer MySQL-Datenbank, die man zunächst anlegen muss. Um sich mit dem System vertraut zu machen, sollte der Benutzer die Bei-

spieldaten herunterladen. So bekommt er gleich das richtige Gespür dafür, wie sich Back- und Frontend „anfühlen“. Die Datensätze sind SQL-Dateien, die man in die zuvor erzeugte Datenbank importiert. (Verwendet man die Beispieldaten nicht, generiert Magento die benötigten Tabellen während der Installation automatisch.)

Während der Installation prüft das Shopsystem auf eventuell fehlende PHP-Extensions und mahnt sie an – im Test waren das *mcrypt* und *curl*.

Nachdem man die fehlenden Extensions in der *php.ini* nachgeladen hat, führt ein Assistent durch die weiteren Installationsschritte. Etwas irritierend ist hier, dass die Shop-Software nicht auf das Vorhandensein von Datenbanktabellen hinweist, wenn die Beispieldatensätze installiert sind. Am Ende der Installation erhält der Benutzer einen sogenannten Encryption Key, den er in jedem Fall notieren sollte. Mit ihm lassen sich später Passwörter et cetera wiederherstellen.




**Magento weist den Benutzer auf fehlende PHP-Extensions hin (Abb. 1).**

## Funktionsumfang erweitern

Magento ist durch allerlei Extensions erweiterbar. Dabei folgen die Magento-Entwickler einem interessanten Konzept: Sie stellen mit Magento Connect einen Marktplatz für Extensions bereit. Dort kann jeder nach der gewünschten Erweiterung suchen und sich über *Get extension key* einen Schlüssel für sie anzeigen lassen. Diesen kopiert man und fügt ihn im Magento Connect Manager ein, den man im Backend über *System/Magento Connect/Manage Extensions* erreicht. *Install* baut eine Verbindung zum Server auf, lädt die Extension und installiert sie.

Innerhalb des Bereichs *Settings* lässt sich zudem noch festlegen, ob die Software ausschließlich Stable-, Beta- oder Alpha-Erweiterungen installieren soll – für den Produktionseinsatz dürften allerdings ausschließlich Stable-Erweiterungen infrage kommen. Zum Testen der Extension-Funktion kann man den Schlüssel *magento-core/Locale_Mage_Core_de_DE* verwenden. Er sorgt für die Anzeige einer deutschsprachigen Magento-Oberfläche. Kleiner Wermutstropfen: Noch ist nicht die gesamte Oberfläche übersetzt. Auch wirken einige Übersetzungen wie *Newsletter Warteschlange* etwas holprig.

Besonders lohnend für Umsteiger vom bisherigen Shop-Platzhirsch osCommerce dürfte sicherlich das osCommerce Migration Tool sein. Dank dieser Erweiterung lassen sich die Daten aus einem osCommerce-basierten Shop holen und in Magento einspielen. Dazu muss der Anwender lediglich IP-Adresse und Zugangsdaten der entsprechenden osCommerce-Datenbank angeben. Den Rest übernimmt das Migrations-Werkzeug. Eine manuelle Kontrolle der importierten Daten ist allerdings unerlässlich.

## Flexibilität durch Templates

Um das Design des Shops so flexibel wie möglich zu gestalten, haben die Entwickler auf ein Template-System gesetzt. Es lässt sich ebenfalls als Extension integrieren und über das Backend aktivieren. Ähnlich wie bei anderen Systemen (ob Shop oder CMS), ist eine Zunahme der Angebote für vorgefertigte Templates abzusehen. Wer das

gewisse Etwas sucht, wird allerdings nicht um das Anlegen eines eigenen Templates herumkommen. Nötig sind dafür Kenntnisse in (X)HTML, CSS, XML und PHP. Um einen Eindruck davon zu vermitteln, wie Templates aussehen, hier ein kleines Beispiel.

```
<reference name="head">
  <action method="addCssle"> ⏎
                              <link>style.css</link>
  </action>
</reference>
```

Durch den Einsatz der *addCssle*-Methode lassen sich CSS-Dateien in Abhängigkeit des verwendeten Browsers laden. Der durch *addCssle* generierte Frontend-Code sieht folgendermaßen aus:

```
<!–[if IE]>>
<link rel="stylesheet" type="text/css" media="all" ⏎
   href="http://www.ourstore.com/skin/frontend/ ⏎
              default/default/css/style.css" ></link>
<![endif]–>
```

Auf diese Weise kann man individuell zugeschnittene Templates erstellen. Negativ fällt bei dem mit Magento ausgelieferten Standard-Template allerdings auf, dass es – obwohl in der Document Type Definition (DTD) *XHTML 1.0 strict* steht – den Standard nicht einhält. Dabei ließe es sich durchaus XHTML-konform gestalten, wenn solche offensichtlichen Mängel wie fehlende *alt*-Attribute für Grafiken und Ähnliches behoben sind. Sollten die Entwickler das Template nicht entsprechend anpassen, kann man das auch selbstständig in den Template-Dateien tun.

## Ein Blick ins Backend

Bereits beim ersten Kontakt zum Backend erkennt man, dass das ganze System sehr übersichtlich gestaltet ist. Der erste Weg sollte in die Konfiguration (*System/Konfiguration*) führen, in der man die grundlegenden Funktionen einstellen kann. Neben allerlei allgemeinen Informationen lassen sich dort auch die beiden Bezahlsysteme Paypal und Googles Checkout konfigurieren.

Für die Betreuung professioneller Shops sind normalerweise mehrere Personen zuständig. Damit sich die einzelnen Backend-Benutzer nicht in die Quere kommen und tatsächlich nur auf die Bereiche zugreifen, die für sie gedacht sind, gibt es ein ausgeklügeltes Benutzergruppensystem. Für jede Gruppe lässt sich detailliert festlegen, welche Backend-Strukturen sie nutzen darf.

Neben dem erwähnten CMS existiert ein Newsletter-Modul für Kunden oder Interessenten. Auch andere Standardfunktionen von Shop-Systemen sind in Magento vorhanden, etwa verschiedene Währungen, Staffelpreise, Googles Sitemap sowie eine übersichtliche Produkt- und Attributverwaltung.

Ebenfalls ausgeklügelt ist die Übersicht über die Verkäufe. Denn schließlich hilft die beste Shop-Software nichts, wenn man nicht detailliert sieht, was Kunden bestellt haben. Darüber hinaus lassen sich Rechnungen verschicken und ausführliche Reports anzeigen. Gerade den Reports sollte ein Shopbetreiber große Aufmerksamkeit widmen, da sich darüber direkt ablesen lässt, wo der Shop noch Potenzial hat. So kann er beispielsweise gezielt nachvollziehen, wie viele Warenkörbe letztendlich nicht bestellt wurden.

## Was der Kunde sieht

Entscheidend dafür, ob die Wahl auf Magento fällt, ist unter anderem der Aspekt der Benutzerfreundlichkeit. Als Kunde kommt man zu dem gewünschten Artikel entweder über die integrierte Suchfunktion oder durch Produkt-Tagging und Produktvergleich. Zudem helfen Produktbewertungen anderer Kunden und weitere Vorschläge bei der Kaufentscheidung. Für diejenigen, die sich nicht sofort für den Kauf entscheiden können, gibt es den Wunschzettel. Dort lassen sich Produkte „parken“. Möchte man sie später tatsächlich kaufen, überträgt man sie einfach vom Wunschzettel in den Einkaufskorb.

Magento erzielte im Test gute Geschwindigkeitswerte beim Laden der Produktinformationen. Allerdings kann man – zumindest wenn man einen eigenen Server betreibt – so einiges für eine höhere Performance tun. Zunächst einmal sollte der Betreiber sicherstellen, dass innerhalb der Apache-Konfiguration *KeepAlives* aktiviert ist. Dadurch können mehrere Anfragen über dieselbe TCP-Verbindung gesendet werden, was zu einer deutlichen Beschleunigung des Seitenaufbaus führt. Weitere Geschwindigkeitsvorteile lassen sich durch den Einsatz von APC, XCach oder anderer PHP Opcode Cacher erzielen.

### Daten und Preise

**Magento-Webshop-System**

Systemanforderungen: Linux, Apache 1 oder 2, PHP 5.2 (oder neuer), MySQL 4.1.2 (oder neuer), Sendmail-kompatibler MTA

Lizenz: Open Software License

Die offizielle Seite: www.magentocommerce.com

Offizieller deutschsprachiger Blog: www.magentocommerce.com/de

## Fazit

Im Gegensatz zu vielen anderen Open-Source-Projekten steht hinter Magento mit Varien ein Unternehmen mit gewachsener Struktur, Venture Capital und allem, was dazugehört. Diese Professionalität ist für (angehende) Shopbetreiber unter Umständen ein Entscheidungskriterium. Denn wer möchte sein Geschäft auf Basis eines neuen Open-Source-Projekts aufbauen, von dem er nicht weiß, ob es in drei Monaten noch weiterentwickelt wird?

Da Magento sehr neu ist, fällt das Angebot verfügbarer Erweiterungen und Templates derzeit noch recht bescheiden aus. Wer sich aber an die Anfänge von vergleichbaren anderen Systemen erinnert, weiß, wie schnell freie Entwickler und kommerzielle Anbieter nachziehen können.

Zum Schluss stellt sich noch die für einen Shop überlebenswichtige Frage nach der Suchmaschinentauglichkeit. Auch hier gibt es Positives zu vermelden. Denn Magento unterstützt die wichtigsten Elemente der On-Site-Optimierung. Überdies generiert die Software aus den Produktdaten sprechende URLs und vergibt logische Seitentitel für die Produktseiten. (ur)

DANIEL KOCH

arbeitet als freiberuflicher Entwickler und Autor.

### iX-Wertung

⊕ großer Funktionsumfang und erweiterbar

⊕ einfache Migration von osCommerce

⊕ übersichtliche Gestaltung

⊖ voller Funktionsumfang nur unter Linux

⊖ deutsche Übersetzung unvollständig und holprig

⊖ standardmäßig keine Validierung nach XHTML 1.0



Tarox’ Parx Server Center 6000R

# RZ in 6HE

**Ralph Hülsenbusch**

Die technische Entwicklung verführt dazu, immer mehr Leistung und Speichervolumen auf kleinem Raum unterzubringen. Was heute in sechs Höheneinheiten passt, zeigt Intels Modular Server. Tarox vertreibt ihn als Parx Server Center und stellte sich als Erster einem Test im *iX*-Labor.

Seit die Prozessoren schrumpfen, die Speicherriegel auf mehrere Gigabyte pro Modul angewachsen sind und die Chip-Sets nahezu alles, was ein Server braucht, on-board unterstützen, erliegen die Designer der Versuchung, Server auf kleinstem Raum unterzubringen. Nach den klassischen Rack-Systemen, die sich auf eine Höheneinheit beschränken konnten und ein wenig an die flachen Pizza-Boxen aus früheren Unix-Workstation-Zeiten erinnern, folgten High-Density-Blades [1] und 1U-Boxen mit Dual-Servern [2]. Nun hat Intel das Konzept des „Modular Server“ hinzugefügt, eine Box, in der sechs „Blades“ samt Massenspeicher Platz finden.

Vor Jahren hatte die Chip-Schmiede zusammen mit IBM intensive Entwicklungsarbeit in das „Blade Center“ gesteckt [3], das bei Intel als Building Block nach wie vor zu haben ist und viele OEMs im Programm haben. Der Modular Server als Produkt für mittelständische Unternehmen traf bei den Anbietern sofort auf Gegenliebe. Einer der ersten, der ein solches System zum Test anbot, war Tarox, ein Systemhaus in Lünen bei Dortmund.

Ein Unterschied zu herkömmlichen Blade-Systemen, der sofort ins Auge fällt, sind die Plattenstapel, die gut ein Drittel der Breite des sechs Einheiten hohen Gehäuses belegen und in der Summe für fast 2 Terabyte (1,89 TByte) Daten Platz bieten (siehe Aufmacher). Die Server-Module stecken waagerecht im Gehäuse, bei Blades bis dato nur in den Telko-Varianten wie dem Blade Center T von IBM üblich.

**iX-TRACT**

- Mit dem Modular Server hat Intel ein RZ in a box realisiert.
- In einem sechs Einheiten hohen Rack-Gehäuse sind sechs Rechner, 14 Platten und die gesamte Netzwerk-Topologie untergebracht.
- Zur Überwachung und Konfiguration dient ein spezielles Modul, das eine Oberfläche nebst Hilfetexten bereitstellt.

## Server in spezieller Bauform

Eine weitere Eigenart zeigt sich beim Blick unter die Haube der Server-Module (siehe Abbildung 1): Die Motherboards tragen Multi-Core-Xeon-Prozessoren, können bis zu 32 GByte FBDIMM-Speicher aufnehmen und nutzen den 5000P-Chipset (Blackford) [4]. Die Anschlüsse auf der Rückseite führen auf eine passive Backplane für die im Gehäuse integrierten LSI-SAS- und die beiden Gigabit-LAN-Controller, Letztere lassen sich per Piggy-Pack auf zwei weitere ausbauen. Auch wenn Farbgebung und Mechanik der Module wie bei den Blades von Intel aussieht – die Server-Module haben im Unterschied zu den Blades weder PCI-Steckplätze noch Raum für lokale Festplatten.

Dreht man das Gehäuse, was man virtuell im Browser auf der Administrationsoberfläche (siehe Abbildung 2) anschaulich nachvollziehen kann, sieht man, dass die Modularität ebenso für Lüfter, Netzteil, Switch-, Speicherkontroll- und Verwaltungsmodul gilt (siehe Abbildung 3). Alles ist redundant einbaubar – bis auf eine Ausnahme: das Verwaltungsmodul, über das der Admin das System remote im Griff hat, gibt es nur einmal. Ein Single Point of Failure, der in erster Linie dem Systemadministrator das Leben schwer machen kann. Das Admin-Netz lässt sich allerdings getrennt vom produktiven führen (out-of-band) – im Gegensatz zu VPro.

## Per Web immer im Bild

Ansprechend und auf den ersten Blick übersichtlich wirkt die Administrationsoberfläche, per HTTPS in jedem Browser erreichbar (siehe Abbildung 4). Die virtuellen Konsolen oder seriellen Verbindungen braucht Java ab Version 1.6 und unter Windows DirectX. Bei der Gestaltung der Oberfläche haben die Entwickler sich offensichtlich aufs Visuelle konzentriert. Erfahrene Administratoren dürften sich auf die Textinfor-



**Volle Packung: In einer „Blade“ sind zwei Xeon-CPUs mit insgesamt acht Kernen am Werk. Da sind acht 1-GByte-Speichermodule fast schon zu wenig (Abb. 1).**

mationen stützen wollen und den Spielereien wie grafisch gezeigten Voltmetern weniger Wert beimessen.

Es gibt über 659 Ereignisse, für die autorisierte Verwalter Policies festlegen können, die beziehen sich aber nur auf das Aktivieren der Überwachung per Log, E-Mail oder SMTP sowie das Exportieren als XML- oder CSV-Datei.

## Heterogene Server im Stapel

Tarox hatte für sein Server Center drei Rechner-Module geliefert, jeweils ausgestattet mit 8 GByte RAM. Komplett bestückt war der Plattenstapel mit 14 SAS-Platten im 2,5-Zoll-Format, jede 140 GByte groß. Zwei Server hatten 3 GHz schnelle Xeon-Prozessoren vom Typ E5450, einer einen Low-Voltage-Xeon L5420 mit 2,5 GHz an Bord. Vorinstalliert waren Windows Server 2003 R3 SP2 auf dem obersten, SLES10 SP1 darunter – beide in einer 32-Bit-Version – und schließlich VMwares ESX Server 3.5. Bei den virtuellen Maschinen fiel die Wahl im Test auf Suse Linux 10.3, Windows Server 2008 und Solaris x86.

Damit bot sich die Gelegenheit, unter anderem zu untersuchen, wie weit die Energieeinsparung zu Lasten der Leistung gehen. Da die logischen Laufwerke mit ihrer Betriebssystemkonfiguration an die Steckplätze der Server gebunden sind, reichte nach dem Herunterfahren ein einfaches Auswechseln der Server, um mit ein und demselben Betriebssystem einen Vergleich mit den CPUs anstellen zu können.

Weitere Aufmerksamkeit gilt aber der Verwaltung des Modular Server. Schließlich muss in der Regel wenig geschultes Personal damit zurechtkommen. Mit ein wenig Obacht gelingt wohl jedem, der mit Volumes, RAID und logischen Laufwerken etwas anfangen kann, das Einrichten eines Servers, vorausgesetzt er hat ein externes USB-Laufwerk oder ein Installations-Image im Netz zur Verfügung. Im letzten Fall kann er den gesamten Prozess aus der Ferne steuern. Es gelingt sogar mit einem remote eingebundenen DVD-/CD-ROM-Laufwerk am Arbeitsplatz, was aber je nach Anbindung viel Zeit beanspruchen kann.

Ärger kommt auf, wenn man die Java-Konsolen für die Server nutzen möchte. Nicht nur, dass die Entwickler die Tastatur unvollständig implementiert haben – der Treiber prellt, sodass man mit einem Tastendruck ganze Ketten von Zeichen erzeugt. Der genervte Anwender sitzt vor einer Konsole, die über Funktionstasten aktivierbar sein soll, die aber nur lokal reagieren. Zum Beispiel bei ALT+SHIFT+F1, bei dem, statt unter Linux in die Konsole umzuschalten, die Help-Funktion des Windows-Client aufpoppt. Besser geht es auf jeden Fall mit einem Remote-Desktop direkt zum Server, bei VMware mit dem Infrastructure Client.

Etwas Umsicht und eine vernünftige Aufteilung der Ressourcen muss man beim Zusammenstellen des Massenspeichers walten lassen. Für Windows hatten die Techniker bei Tarox ein RAID 60 (RAID 6 gespiegelt) mit 100 GByte angelegt, für Linux ein 135 GByte großes RAID 6. Auf dem ESX-Server kam ein ebenfalls 135 GByte großer Storage Pool im RAID-6-Verbund zum Einsatz. RAID 6 ist ein Nachkomme von RAID 5 mit doppelten Prüfsummen, verteilt über alle Platten. Es braucht mindestens vier Platten, verkraftet dafür aber den Ausfall von zwei Laufwerken. Der Modular Server bietet die RAID-Level 0, 5, 6, 10, 50, 60 und 1E, Letzterer spiegelt die Blöcke auf die jeweils nächste Platte im Verbund.

## Xeon mal heiß, mal sparsam

Als Last für den Windows- und den Linux-Rechner diente die CPU2006 der SPEC. Erste Messergebnisse zeigten, dass man den Einsatz der „Sparversion“ des Xeon L5420 durchaus ins Kalkül ziehen kann. Allein vom Prozessortakt aus gerechnet müsste der L5420 nur noch 5/6 (83 %) der Rechenleistung des E5450 erreichen, kommt im Benchmark unter Linux beim Einzellauf auf exakt den Wert,

**Durchblick: Im Browser erkennt der Administrator im Bild, welches Modul er gewählt hat. Ein Klick rechts unterm Bild, und es erscheint die Rückseite des Gehäuses (Abb. 2).**






**Freiräume: Im Testgerät waren das Speichermanagement- und das Switch-Modul nicht redundant ausgelegt. Die beiden Lüfter unterhalb der Netzteile lassen sich gegen weitere Netzteile austauschen (Abb. 3).**

im Rate aber auf 99 %, während er unter Windows nur noch 72 % respektive 92 % erreicht. Da kaum jemand die beiden Quad-Core-CPUs nur mit einer einzigen nicht parallelisierbaren Anwendungen nutzen dürfte, ist der Schluss eindeutig: die Low-Voltage-Variante L5420 lohnt sich allein vom Preis her, denn sie ist mit rund 350 Euro pro Chip nur halb so teuer wie der E5450, der mit an die 750 Euro zu Buche schlägt. Aber auch beim Energieverbrauch gibt es Einsparungen: Intel spezifiziert die Xeon-Prozessoren der L5400-Serie mit 50, die der E5400- mit 80 Watt.

Auf dem Dashboard des Web-Interface „Modular Server Control“ hat der Administrator unter anderem den aktuellen Stromverbrauch im Blick und kann dort erkennen, welches Netzteil-Modul welche Leistung erbringt. Sind mindestens zwei eingebaut, liefern beide Strom, sind aber redundant. Fällt eins aus, übernimmt das andere. Leider gibt es nur Wattzahlen für das gesamte System und nicht für die einzelnen Server. Außerdem wären Minimum- und Maximumangaben wünschenswert. Die Sensoren für die jeweiligen Rechnermodule zeigen nur die Spannungstoleranzen an. Wenn jedoch nur eins eingeschaltet ist, kann man zwischen Leerlauf und Last gut unterscheiden. Unter Windows verbraucht der Modular Server mit dem L5420 etwa 250 Watt, unter voller Last steigt der Energiehunger tatsächlich auf runde 350 Watt.




**In Fahrt: Auf dem Dashboard des Web-Client liefert die Modular Server Control einen Überblick des Gesamtsystems. In regelmäßigen Abständen aktualisiert der Webserver die Informationen (Abb. 4).**

## Fazit

Wer ein System sucht, das en bloc alles mitbringt, was für den RZ-Betrieb nötig ist, stößt bei Intels Modular Server auf ein passendes Konzept, das gemessen an seinen Möglichkeiten mit wenig Raum auskommt. Obwohl alles in einem Gehäuse steckt, muss man bei der Ausstattung nicht sparen: sechs Server mit insgesamt 48 Prozessorkernen, 256 GByte RAM, 2 Terabyte auf 14 Festplatten und zehn 1-Gigabyte-Ethernet-Ports dürften für fast alle Szenarien in kleinen und mittleren Unternehmen oder Filialen ausreichen.

Bei der Administration gibt es zwar kleine Einschränkungen, dafür haben die Designer eine übersichtliche und intuitiv bedienbare Oberfläche geschaffen, die selbst bei langsamen Verbindungen noch mitspielt. Bei kritischen Fällen dürfte die Refresh-Rate von rund 1 Minute etwas zu langatmig sein, und die im Control Center gebotenen Java-Konsolen sind eine Qual.

Intel hat versucht, konsequenter als bei den Blades ein Konzept zu verwirklichen, um kleinen und mittlere Unternehmen sowie Außenstellen etwas anzubieten, das in einem Gerät sämtliche IT-Aufgaben erledigen kann und das wenig Schulungsaufwand für die Grundadministration erfordert. Das ist gelungen. (rh)

### Ergebnisse der CPU2006

| | L5420 (Linux) | E5450 (Linux) | L5420 (Windows) | E5450 (Windows) |
|---|---|---|---|---|
| SPECint_base2006 | 15,9 | 16,3 | 11,8 | 16,2 |
| SPECint_rate_base2006 | 82,5 (64 %) | 82,7 (63 %) | 44,7 (47 %) | 48,1 (37 %) |
| SPECfp_base2006 | 14,1 | 15,8 | 1 | 1 |
| SPECfp_rate2006 | 58,6 (51 %) | 62,4 (49 %) | 1 | 1 |

Intels Compiler Suite Version 10, Option *–fast*;
Linux: SLES10 SP1; Windows: 2003 Server;
[1] Fortran-Tests mangels ausreichenden Speichers nicht lauffähig

**Lastenträger: Obwohl die L5420-CPU ein Sechstel langsamer getaktet ist, fällt sie hinter der E5450 nur wenig zurück (Abb. 5).**

### iX-Wertung

⊕ hohe Ausbaubarkeit
⊕ intuitive Bedienung
⊕ leichtes Auswechseln der Komponenten
⊖ fehlerhafte Java-Konsolen
⊖ unüberschaubare Zahl von Ereignissen bei den Policies

### Lieferumfang und Preise

**Parx Server Center 6000X** Modular Server
**Hardware** pro Server: bis zu zwei Xeon-Multi-Core-CPUs, maximal 32 GByte FB-DIMM
**Speichermodul:** 14 Slots für 2,5-Zoll-Platten, RAID 0, 1, 6, 10, 1E, 60
**Switch-Modul:** zehn externe Gigabit-Ports, 12 interne
**Management-Modul:** 100-MBit-Ethernet-Port fürs Verwaltungsnetz, integrierter Webserver
**Gehäuse:** bis zu vier Netzteile, zwei Hot-Swap-Hauptlüfter, ein Hot-Swap-I/O-Lüfter (zwei Netzteile durch Lüftermodule ersetzbar)
**Software:** Modular Server Center, Java-Clients für Remote KVM
**Hersteller:** Intel; www.intel.com
**Anbieter:** Tarox, Lünen; www.tarox.de
**Preis:** auf Anfrage

## Literatur

[1] Axel Urbanski; Blades; Sparschweine im Doppelpack; High-Density-Blades mit stromsparenden CPUs: HS420 von Nexcom; *iX* 7/2004, S. 70
[2] Harry Schlagenhauf, Steffen Stadel; Number Crunching; Knoten geplatzt; Microsofts High-Performance-Computing: Windows CCS 2003; *iX* 9/2007, S. 64
[3] Ralph Hülsenbusch; Blade-Server; Gesteckte Werte; Modular Power: Blade-System auf Intel-Basis; *iX* 7/2004, S. 63
[4] Ralph Hülsenbusch; HW-Plattform; Vorläufer; Intels neue Bensley-Plattform unter Linux: RX300 S3 von FSC; *iX* 7/2006, S. 102



FreeBSD 7.0 im Test

# Überholt

**René Keller ,**
**Martin Wundram**

Vor allem Internet-Provider setzen FreeBSD wegen seiner Stärken im Netzwerkbereich häufig ein. Ein Test soll zeigen, ob die mit der Release 7.0 erfolgte kräftige Überarbeitung des Open-Source-Betriebssystems messbare Vorteile bringt.

Im Schatten der allgemeinen Aufmerksamkeit rund um Linux haben die Entwickler FreeBSD 7.0 freigegeben. *iX* hat sich die neue Version genauer angesehen und mit ihrem Vorgänger verglichen.

FreeBSD 7.0 präsentiert sich mit grundlegenden Neuerungen, behält das ein oder andere Relikt aber bei. Das Projekt besteht fast 15 Jahre. Es basiert, wie die verwandten Projekte NetBSD und OpenBSD, auf der Berkeley Software Distribution (BSD) und hat damit seinen Ursprung im AT&T-Unix der 70er-Jahre. Seine Stärken liegen im Netzbereich, es ist schlank, robust und zuverlässig, Internet-Provider setzen es beispielsweise gern ein. Bei Topcraft finden sich unter den Top Ten der Server mit der längsten Uptime (siehe „Onlinequellen, [a]) sieben FreeBSD-Systeme.

In die Release 7.0 sind neben etlichen Bugfixes und routinemäßigen Änderungen sowohl im Kern als auch im Userland zum Teil bedeutende Anpassungen und Erweiterungen eingeflossen [b]. Die neue Version bildet die Basis für die Entwicklung der kommenden Jahre. Die bisherige 6.x-Reihe – aktuell ist 6.3 –, wird jedoch weiter gepflegt. So lassen sich bestehende Installationen, beispielsweise in Serverumgebungen, sicher weiter betreiben.

Ein wichtiges Merkmal der neuen Version 7.0 ist der verbesserte Mehrprozessor-Support. Die Arbeiten, den Kernel zu einem Multi-Thread-System umzugestalten, begannen im Jahr 2000 und gelten nun als fast abgeschlossen. Der Kernel arbeitet vollständig parallel und nur noch sehr wenige Ausnahmefälle erfordern ein sogenanntes „Giant Locking“. Giant Locks, oder generischer Kernel Locks, werden durch den Wechsel vom User- in den Kernel-Modus ausgelöst. Solange eine Aufgabe im Kernel-Modus läuft, ist keine parallele Verarbeitung anderer Aufgaben auf weiteren Prozessoren möglich.

## Neuerungen an der Plattform

Bisher ordnete der Scheduler Prozesse ohne Berücksichtigung eines Bearbeitungszusammenhangs beliebig freien CPU-Kernen zu. Der ULE-Scheduler verwaltet jedoch pro Kern eine eigene Queue und lässt einen Prozess möglichst auf dem zuletzt verwendeten Kern laufen, was einen effizienteren Speicherzugriff ermöglicht. Diese Maßnahmen führten zu einer zum Teil deutlichen Performancesteigerung in Multi-CPU-Systemen. Von den Entwicklern durchgeführte Benchmarks zeigen lineare Skalierung bis 8 CPUs [c]. Inzwischen unterstützt der installierte Standard-Kernel SMP (Symmetric Multiprocessing) und verwendet damit direkt nach der Installation alle erkannten CPU-Kerne.

Mit der Freigabe von 7.0 sind die Entwickler von der 3.x-Reihe der GNU Compiler Collection (GCC) auf 4.2.1 umgestiegen, die OpenMP mitbringt. Für C, C++ und Fortran reduziert sich dadurch der Kodieraufwand für Parallelisierung und Threading deutlich. Außerdem ist der Stack-Smashing-Protector per Default aktiviert. Dadurch lassen sich Pufferüberläufe zur Laufzeit erkennen und Abwehrmaßnahmen umsetzen.

Mit *jemalloc* haben die Entwickler eine neue *malloc*-Implementierung eingebunden. Sie verbessert die Performance von Multi-Threaded-Programmen insbesondere in SMP-Umgebungen, ohne dass Single-Threaded-Anwendungen Einbußen hinnehmen müssen. Davon waren die Firefox-Programmierer so überzeugt, dass *jemalloc* Einzug in Firefox 3 gefunden hat und dort für mehr Geschwindigkeit und weniger Speicherverbrauch sorgt. Der Firefox-Entwickler Stuart Parmenter berichtet in seinem Blog [d] von 22 % weniger Speichernutzung durch *jemalloc* in Windows Vista.

Bei der von OpenBSD portierten Paketfilter-Firewall PF wechselte man von der in OpenBSD 3.7 enthaltenen Version auf die von 4.1. Darüber hinaus unterstützt FreeBSD mit dieser Release erstmalig IPMI (Intelligent Platform Management Interface). IPMI eignet sich beispielsweise für Statusabfragen über den Systemzustand, aber auch zum Einbinden einer seriellen Konsole über das IPMI-LAN-Interface. Das ist vor allem dann praktisch, wenn ein entfernter Server nicht mehr reagiert.

Das Tool *freebsd-update* ermöglicht das Herunterladen, Installieren und Deinstallieren von Binär-Updates für das Basissystem. Die Updates stellt das FreeBSD-Security-Team bereit.

| Messergebnisse | | | |
|---|---|---|---|
| | **FreeBSD 7.0 (ULE)** | **FreeBSD 7.0 (4BSD)** | **FreeBSD 6.3** |
| **MySQL** | | | |
| Threads | Transaktionen/s | Transaktionen/s | Transaktionen/s |
| 1 | 567,03 | **612,93** | 509,79 |
| 2 | **1055,20** | 973,97 | 707,72 |
| 4 | **1012,14** | 947,97 | 670,18 |
| 16 | **938,24** | 808,75 | 579,24 |
| 64 | **761,49** | 747,20 | 471,23 |
| 128 | 386,57 | **394,92** | 287,37 |
| 512 | 233,21 | **237,96** | 109,23 |
| **PostgreSQL** | | | |
| Threads | Transaktionen/s | Transaktionen/s | Transaktionen/s |
| 1 | **539,89** | 495,86 | 450,59 |
| 2 | 682,31 | **795,97** | 650,56 |
| 4 | 693,09 | **811,72** | 644,63 |
| 16 | 681,24 | **725,10** | 584,72 |
| 40 | 649,71 | **661,25** | 564,31 |
| **Threading** | | | |
| Threads | Laufzeit in s | Laufzeit in s | Laufzeit in s |
| 1 | **4,09** | 5,64 | 20,43 |
| 2 | **2,51** | 4,72 | 23,76 |
| 4 | **2,79** | 6,26 | 26,38 |
| 16 | **4,39** | 18,18 | 58,86 |
| 128 | **8,03** | 27,60 | 130,02 |
| 512 | **21,92** | 31,44 | 199,06 |
| **Memory** | | | |
| Threads | Laufzeit in s | Laufzeit in s | Laufzeit in s |
| 1 | 733,63 | **723,51** | 749,84 |
| 2 | 517,44 | **515,85** | 518,22 |
| 4 | 517,29 | **516,05** | 516,82 |
| 8 | 516,62 | **516,03** | 517,44 |
| **Real-Life-Webseite mit 30 parallelen Anfragen** [1] | | | |
| | 3:24 | **3:21** | 3:28 |

[1] Typo3-Webseite www.wim.uni-koeln.de mit 4283 Seiten, Laufzeit in MM:SS

Nichts Neues gibt es bei der Systeminstallation. Das Grundsystem ist zwar in kaum mehr als fünf Minuten eingerichtet. Aber nach wie vor startet die Boot-CD den spartanisch anmutenden Installer *sysinstall*, der textbasiert durch die Installation führt. FreeBSD setzt nun seit über zwölf Jahren auf dieses Werkzeug und der Man-Page ist zu entnehmen: „This utility is […] greatly in need of death.“ Leider haben es die Ergebnisse der Versuche, einen neuen Installer zu entwickeln, noch nicht in die aktuelle Release geschafft. Das ist insbesondere dann ärgerlich, wenn man zum Beispiel schon während der Installation ein Soft-RAID einrichten möchte. *sysinstall* ist hierzu nicht in der Lage und man ist gezwungen, eine Shell zu starten und dort die nötigen Schritte händisch zu erledigen.

## Netzwerkbereich umgekrempelt

FreeBSD 7 bietet einen neuen TCP-Verbindungspuffer. Während die Vorversionen standardmäßig 32 KByte für jede TCP-Verbindung reservierten, steht nun standardmäßig ein bis zu 256 KByte großer Puffer zur Verfügung, dessen Größe FreeBSD automatisch verwaltet. Beim Öffnen einer Verbindung zu einer Remote Shell per SSH alloziert das Betriebssystem beispielsweise weiterhin nur den 32 KByte großen TCP Socket Buffer, beim Transfer einer großen Datei erhöht sich dessen Größe jedoch schnell auf 256 KByte. Die maximale Puffergröße lässt sich in */etc/sysctl.conf* individuell konfigurieren.

Insbesondere bei schnellen Verbindungen mit langen Paketlaufzeiten und hohem Datenvolumen macht sich dies bemerkbar. So ergaben Tests der Entwickler, dass der Transfer einer großen Datei aus USA von einem FreeBSD-Server mit dem neuen TCP Socket Buffer mehr als dreimal so schnell ist.

Weiterhin neu ist die Verarbeitung eingehenden Netzwerkverkehrs. Die neue Architektur übernimmt die komplette Verarbeitung. Während frühere Versionen beim Überlaufen des annehmenden *netisr*-Threads ein Paket verwerfen, stellt FreeBSD 7.0 die Verarbeitung eines einmal angenommenen Datenpakets sicher.

Ein weiterer Geschwindigkeitsvorteil bei Gigabit-Ethernet und schnelleren Karten ergibt sich durch die Unterstützung der Techniken TSO (TCP/IP Segmentation Offload) und LRO (Large Receive Offload). TSO ermöglicht eine Aufspaltung von Netzdaten in einzelne TCP-Pakete direkt auf der Hardware der Netzwerkkarte. LRO spielt seine Stärken insbesondere im LAN aus. Oft verschicken Systeme hier mehrere aufeinanderfolgende Pakete an denselben Adressaten, die sich via LRO zusammenfassen lassen.

Im Drahtlosbereich verbesserte man die Suche nach verfügbaren Netzen. So aktualisiert das System bei Inaktivität im Hintergrund den Cache der verfügbaren Netze und wechselt gegebenenfalls zu einem stärkeren Access Point. Ebenfalls neu ist die Unterstützung des 802.11n-Standards.

Um sich für die Zukunft zu wappnen, aktiviert FreeBSD 7.0 als erstes Betriebssystem standardmäßig die Unterstützung für das SCTP (Stream Control Transmission Protocol). Es gilt als Nachfolger der auf dem Internetprotokoll (IP) aufsetzenden Protokolle TCP und UDP. SCTP ist bereits in professionellen innerbetrieblichen Kontexten häufiger im Einsatz und dürfte sich aufgrund seiner Vorzüge schnell verbreiten. Diese liegen unter anderem in der Übertragung transaktionsbasierter Daten – wichtig beispielsweise bei Onlinebanking-Anwendungen – und in einer besseren Fehlerbehandlung bei unzuverlässigeren Verbindungen, wie es bei mobilen Verbindungen der Fall ist. Die Optimierung von FTP-, SSH- und HTTP-Applikationen ist schon in Arbeit.

## Softwareverwaltung via Ports-System

FreeBSD speichert die zur Verfügung stehende Software in sogenannten Ports. Eine Stärke dabei: Software ist in der Regel nicht an die Betriebssystemversion gebunden, womit auch ältere Installationen leicht in den Genuss neuer Anwendungen kommen können. Die Liste zur Verfügung stehender Ports erweitert sich ständig und lag bei der Release von FreeBSD 7.0 bei circa 18 000 – rund 1700 mehr als in FreeBSD 6.2. KDE4 gehört noch nicht zum offiziellen Umfang, die Integration macht aber Fortschritte. OpenSSH liegt in Version 5.0 vor und unterstützt nun das „Einsperren“ von Benutzern in bestimmte Verzeichnisse. Binär-Pakete aus der 6.x-Reihe lassen sich via *compat6x*-Tool weiterverwenden.

Software, die nicht als FreeBSD-Port zur Verfügung steht, beispielsweise der Acrobat Reader oder das Flash-Plug-in, kann man im Linux-Kompatibilitätsmodus betreiben. Standardmäßig emuliert der sogenannte *linuxulator* einen Linux-Kernel in der Version 2.4.2. FreeBSD 7.0 liefert ebenfalls eine 2.6er-Emulation

(2.6.16), diese läuft jedoch noch nicht bei allen Anwendungen stabil.

FreeBSD 7.0 bietet mit *gjournal* einen vom Dateisystem unabhängigen Journal-Provider, mit dem das standardmäßig genutzte Unix File System (UFS2) zum transaktionssicheren Dateisystem mutiert. Intelligente Caching- und Optimierungsalgorithmen verbessern zudem die UFS2-Performance. Beispielsweise versucht *gjournal* einzelne kleine Anfragen zu größeren zu kombinieren, um Disk-I/O zu minimieren und die Daten so zu sortieren, dass deren Lage die Kopfsuchzeiten minimiert.

Neu ist das von NetBSD portierte *tmpfs*. Es ermöglicht RAM-Disks mit dynamischer Größe. Allerdings stürzte FreeBSD 7.0 bei den Tests beim Verschieben von Dateien in einer *tmpfs*-Partition reproduzierbar hart ab.

Eine weitere GEOM-Neuerung – GEOM ist ein seit der Version 5.0 verfügbares modulares Speicher-Framework – ist *gvirstor*. Mit ihr lässt sich ein virtueller Datenträger beliebiger Größe erstellen und auf mehrere physische Datenträger verteilen. Dabei kann zum einen die Größe des virtuellen Datenträgers die physische Gesamtgröße überschreiten und zum anderen lassen sich im laufenden Betrieb Datenträger hinzufügen und entfernen.

Darüber hinaus beherrscht FreeBSD 7 Suns Dateisystem ZFS, UnionFS sowie nur lesend XFS. Außerdem beherrscht der in Version 6.0 eingeführte parallele Zugriff auf UFS-Dateiverwaltungssysteme nun auch die parallele Verarbeitung von Quotas. Der Zugriff auf NFS-Systeme erfolgt jetzt auf Server- und Client-Seite parallelisiert, was sich positiv auf die Geschwindigkeit bei Mehrprozessorsystemen auswirkt.

Im Wesentlichen lassen sich die Leistungsverbesserungen (siehe Tabelle „Messergebnisse“) auf die neue Netzwerkarchitektur, das neue Threading-Modell zurückführen. Das neue 1:1-Threading-Modell bietet in Verbindung mit dem verbesserten Speichermanagement für SMP-Systeme signifikante Performancevorteile bei Applikationen, die kleine Speicherbereiche pro Thread reservieren (siehe die MySQL- und PostgreSQL-Tests in der Tabelle).

Eine weitere Möglichkeit zur Leistungssteigerung ist der neue optionale ULE-Scheduler. Die drei Buchstaben stehen dabei lediglich für den Schluss von „Schedule“. Der ULE-Scheduler bietet diverse Vorteile, indem er durch Heuristiken interaktive Prozesse erkennt und sie priorisiert einplant. Weiterhin verwaltet er eine Scheduling-Liste pro CPU und berücksichtigt CPU-Eigenschaften. Davon profitieren nach Aussage der Entwickler vor allem Anwendungen mit vielen zusammenarbeitenden Threads, wie Windows-Manager.

### iX-Wertung

⊕ gute Netzwerk-Performance
⊕ effiziente Softwareverwaltung
⊕ schlankes Basis-System

⊖ Installationsroutine nicht zeitgemäß
⊖ Hardwareunterstützung nicht so umfangreich wie bei Windows/Linux

### Onlinequellen

| | | |
|---|---|---|
| [a] | Netcraft Top Ten Uptime | uptime.netcraft.com/up/today/top.avg.html |
| [b] | FreeBSD-7.0-Neuerungen | www.freebsd.org/releases/7.0R/relnotes.html |
| [c] | ULE-Skalierung | people.freebsd.org/~kris/scaling/7.0%20Preview.pdf |
| [d] | Stuart Parmenter | blog.pavlov.net/2008/03/11/firefox-3-memory-usage/ |

## FreeBSD im Leistungsvergleich

Tests der Entwickler zeigen, dass sich bei Mehrprozessormaschinen mit mehr als vier Prozessoren signifikante Performancesteigerungen im Vergleich zum BSD-Scheduler realisieren lassen.

Für diesen Artikel führten die Autoren einen Performancevergleich der FreeBSD-Versionen 6.3 und 7.0 durch, Letztere je einmal mit dem normalen 4BSD- sowie dem ULE-Scheduler. Als Hardware-Grundlage diente gezielt ein Allzweck-Webserver, wie er oft im ISP-Bereich zum Einsatz kommt: ein Dual-Core Athlon64 X2 4600+ (2,4 GHz) mit 4 GByte RAM. I/O-kritische Bereiche des Dateisystems liefen von einer RAM-Disk aus. Insbesondere die Datenbankdaten standen damit I/O-unkritisch zur Verfügung. Als Benchmark diente die *sysbench*-Suite. Ein weiterer Real-Life-Performancetest bestand im Betrieb einer umfangreichen Typo3-Website mit knapp 4300 Seiten, die 30 parallele Anfragen zu bedienen hatte.

Zwei deutliche Ergebnisse lieferten die Tests: FreeBSD 7.0 erreicht in allen durchgeführten Benchmarks mehr Geschwindigkeit als 6.3, aber der ULE-Scheduler ist nicht in allen Fällen schneller als der bewährte 4BSD-Scheduler. Zwar resultiert der ULE-Scheduler bei 7.0 in einem Performancegewinn im MySQL- und in deutlichen Unterschieden im Threading-Benchmark. Die PostgreSQL- und Sysbench-Memory-Tests entscheidet allerdings das System mit 4BSD-Scheduler für sich. Zum Teil deutlich geschlagen geben muss sich Version 6.3 trotz ebenfalls vorhandener SMP-Unterstützung.

Den Praxistest konnte ebenfalls FreeBSD 7.0 für sich entscheiden. Allerdings siegte hier der 4BSD-Scheduler vor dem ULE-Scheduler, gefolgt von dem 6.3er-System. Insgesamt lagen die Testergebnisse aber nahe beieinander. Während FreeBSD 7.0 mit 4BSD-Scheduler die 4283 Webseiten in 3 Minuten und 21 Sekunden lieferte, brauchte der ULE-Scheduler 3 Sekunden und das 6.3er-System 7 Sekunden länger für diesen Job.

## Fazit

Mit FreeBSD 7.0 erhält man ein schlankes, performantes und effizient zu administrierendes System aus einem Guss. Dank verbessertem Threading-Modell und überarbeiteter Netzwerkarchitektur bietet die neue Version gegenüber der 6er-Reihe deutliche Geschwindigkeitsvorteile. Den Einsatz des neuen ULE-Schedulers sollte man im Einzelfall vom Nutzungs- und Hardware-Szenario abhängig machen. (avr)

MARTIN WUNDRAM

ist Geschäftsführer der *TronicGuard GmbH* und als Sachverständiger und Trainer für Computersicherheit und -forensik tätig.

RENÉ KELLER

ist Geschäftsführer der *explicatis internet und systemlösungen gbr* und Doktorand am Seminar für Wirtschaftsinformatik und Informationsmanagement der Universität zu Köln.








Netbeans 6.1: Es gibt nicht nur Eclipse

# Zweiter Frühling

**Markus Stäuble**

Im Schatten des Eclipse-Projekts hat sich Netbeans zu einer ernstzunehmenden Alternative in Sachen Java-Entwicklung gemausert. Zwar verfügt das Werkzeug nicht über Wunderfunktionen, gefällt aber im Detail.

Netbeans startete 1996 als Studentenprojekt in der Tschechischen Republik zunächst unter dem Namen Xelfi (in Anlehnung an Delphi von Borland). Es war die erste Entwicklungsumgebung für Java, die komplett mit ebendieser Sprache entwickelt wurde. Der heutige Name resultierte aus dem ehrgeizigen Plan, netzwerkfähige Java-Bean-Komponenten, sogenannte Netbeans, entwickeln zu können. Nachdem Sun den ersten Entwurf seiner Enterprise Java Beans verabschiedet hatte, entschloss sich das Netbeans-Entwicklerteam, von seiner eigenen Beans-Variante Abschied zu nehmen, und setzte auf den EJB-Industriestandard.

Wer die neue Version 6.1 ausprobieren möchte, muss zunächst aus sieben Paketen das passende heraussuchen. Es existieren Ausführungen für Web & Java EE, Mobility (nicht für Mac OS X und Solaris), Java SE, Ruby, C/C++, Early Access for PHP (erste Version der PHP-Unterstützung) sowie das Komplettpaket „All“, das neben der IDE den Applikationsserver Glassfish und den Servlet Container Apache Tomcat enthält (alle Downloads über den *iX*-Link am Textende oder Kasten „Onlinequellen“). Die 183 MByte große Windows-Variante des Letzteren ließ sich unter XP mit Java 6 ohne Schwierigkeiten installieren. Nach dem Start präsentiert Netbeans eine Willkommensseite, die an den Konkurrenten Eclipse erinnert und einige Einstiegshilfen bereithält (Abbildung 1).

Bei der Anlage eines Projekts (*File -> New Project*) muss man aus einer Liste (Java, Web, UML, Ruby …) das Gewünschte auswählen. Ein Debugger hilft bei der Fehlersuche und der Analyse des Quellcodes. Die wichtigen Breakpoints setzt der Programmierer per Klick am linken Zeilenrand. Er kann sie mit einer Bedingung (programmiert in Java) versehen (über Kontextmenü am Breakpoint: *Breakpoint -> Customize*). Der Editor verfügt wie alle anderen über eine Code-Vervollständigung. Erst beim Eintreten einer Bedingung schaltet sich der Debugger ein, was besonders bei großen Schleifen hilfreich ist. Die Breakpoints lassen sich in einer separaten Ansicht betrachten (*Window -> Debugging -> Breakpoints*). Neben der genannten Möglichkeit, einen Breakpoint in einer Klasse zu setzen, geht das auch über *Run -> New Breakpoint*. Der zugehörige Dialog bietet zahlreiche Optionen, zum Beispiel das Setzen eines Breakpoint beim Auftreten einer Exception (über *Breakpoint Type*).

## Überwachung wird großgeschrieben

Der Profiler offeriert drei Analysemodi: CPU Profiling, Memory Profiling und Thread Monitoring (Abbildung 2). Zum Untersuchen einer Anwendung wählt der Entwickler über das Kontextmenü der jeweiligen Startklasse den Punkt *Profile File* aus. Während des Analysevorgangs kann er Snapshots erzeugen. Am Ende der Anwendung macht der Profiler ebenfalls einen Schnappschuss. Anhand dieser Momentaufnahmen lassen sich kritische Stellen und Performancefresser aufspüren.

Jede Entwicklungsumgebung benötigt für die Verwaltung der Projekte einen Satz an Metadaten. Netbeans speichert die beschreibenden Informationen in Property- und XML-Dateien. Die verschiedenen Aktionen im Entwicklungsprozess (zum Beispiel JUnit-Tests) startet Netbeans über Skripte. Dahinter steht das Build-System Apache Ant. Vorteil: Das Projekt lässt sich ohne IDE übersetzen. In Konkurrenzwerkzeugen muss man sich diese Möglichkeit mühsam selbst basteln. Nachteil: Einige Plug-ins, etwa Checkstyle, geben ihre Meldungen nur textuell auf der Konsole aus. Das kann Eclipse besser, es schickt Meldungen von Plug-ins immer an die entsprechenden Views.

Neben vielen Wizards und Erweiterungen für die verschiedenen Frameworks legt die IDE gegenüber älteren Versionen eine zumindest subjektiv

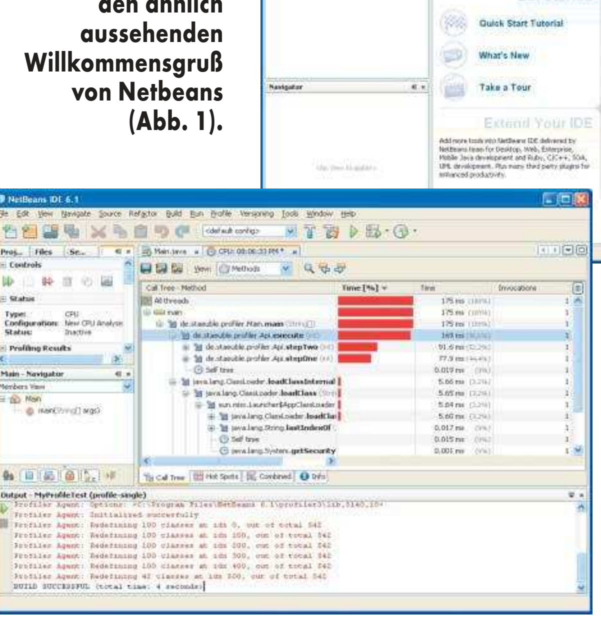
bessere Gesamtperformance an den Tag. Das Fenstersystem ist nun ähnlich komfortabel wie das von Eclipse. Beispielsweise erhält man beim Verschieben von Fenstern eine transparente Vorschau des Layouts.

## Gutes RAD ist nicht teuer

Für das sogenannte Rapid Application Development (RAD) bringt Netbeans 6.1 ebenfalls einiges an Rüstzeug mit. Dazu gehört zunächst einmal die Unterstützung des Swing Application Framework (JSR 296) in Verbindung mit der Beans Binding Technology (JSR 295), über die sich beispielsweise Datenbanken automatisch anbinden lassen. Für diese Kombination existiert ein eigener Projekttyp namens Java Desktop Application. Mit dem GUI-Editor Matisse erzeugt der Entwickler die grafischen Oberflächen. Er benutzt dazu entweder die bekannten Komponenten von Swing (etwa JFrame), modifizierte Varianten davon oder selbstgeschriebene Module. Swings Layout-Manager hilft bei deren Anordnung; eine absolute Platzierung ist ebenfalls möglich.

Generierter Code muss immer mit dem selbstgeschriebenen synchronisiert werden, was oft zu Schwierigkeiten führt. Matisse erlaubt das Programmieren von Funktionen nur in bestimmten Bereichen, die generierten Teile sind schreibgeschützt. Der Mechanismus gewährleistet, dass sich der Code nach manuellen Änderungen weiterhin im grafischen Editor bearbeiten lässt.

Netbeans ist mit Plug-ins erweiterbar. Über den Menüpunkt *Tools -> Plugins* verwaltet und installiert der Anwender die gewünschten Module (Dateiendung *.nbm*). Der Javascript-Editor basiert nun wie der von Ruby auf Netbeans Generic Scripting Framework (GSF) und bietet entsprechenden Komfort, etwa Code-Vervollständigung und kontextsensitive Dokumentation. Der Kauf von MySQL durch Sun wirkte sich auf die vorliegende Netbeans-Version aus: Sie arbeitet nun mit der Datenbank zusammen und verfügt beispielsweise über Funktionen zum Starten und Stoppen des MySQL-Servers.



**Hier handelt es sich nicht um die Einstiegsseite von Eclipse, sondern um den ähnlich aussehenden Willkommensgruß von Netbeans (Abb. 1).**

**Via CPU Profiling erfährt der Entwickler, wie viel Zeit die einzelnen Methoden benötigen. Über den Reiter Hot Spots gelangt er direkt zu den kritischen Stellen im Code (Abb. 2).**

Da sich die heute angebotenen Entwicklungsumgebungen nicht fundamental unterscheiden, muss der Interessent bei den Details suchen. Netbeans 6.1 kommt nicht mit dem großen Sack an neuen Ideen, aber Dinge wie der integrierte Profiler oder der Interface-Designer Matisse verstehen zu gefallen. Alle Standards, die man heute von einer IDE verlangen kann (etwa Code-Komplettierungen, Debugger, gute Navigation innerhalb des Quellcodes) sind umgesetzt.

## Fazit

Wer sich zwischen Eclipse und Netbeans entscheiden muss, sollte nicht nur auf die technischen Funktionen schauen, sondern auch den Support durch die Community kritisch betrachten. Als klarer Sieger dürfte hier keiner der beiden IDEs vom Platz gehen. Für den einen oder anderen liefern möglicherweise die unterschiedlichen Architekturen (Eclipse RCP mit SWT und OSGi sowie Netbeans auf Basis von Swing und eigenem Plug-in-Mechanismus) bessere Anhaltspunkte für die Auswahl. Da Netbeans 6.1 Eclipse-Projekte importieren kann, steht einem Testlauf nichts im Wege.

Die gute Integration des Swing Application Framework sowie der neu aufgesetzte Javascript-Editor sprechen dafür, sich Netbeans näher anzuschauen. Wer keine allzu großen Ansprüche an seine Java IDE stellt, ist eventuell schon mit der kleinen Ausgabe für Java SE, die lediglich 25 MByte Lebendgewicht auf die Waage bringt, gut bedient. Vor allem dank seiner Fähigkeiten beim Rapid Application Development sammelt das Werkzeug Pluspunkte. Es bietet keine Killerfunktionen, mit denen es andere IDEs locker ausstechen könnte, überzeugt jedoch im Detail. Gemäß Roadmap soll Release 7.0 Ende November dieses Jahres erscheinen. (jd)

### Onlinequellen

| | |
|---|---|
| Homepage Netbeans | www.netbeans.org |
| Plug-ins | plugins.netbeans.org |
| Wiki | wiki.netbeans.org |
| Modulentwicklung | platform.netbeans.org/tutorials/quickstart-nbm.html |
| Apache Ant | ant.apache.org |

### iX-Wertung

⊕ integrierter Profiler sowie GUI-Designer

⊕ gute Javascript-Unterstützung

⊕ Projekterstellung mit Ant

⊖ visuelle Plug-in-Unterstützung

MARKUS STÄUBLE

ist Senior Software Engineer bei der Namics (Deutschland) GmbH.



iX-Link ix0807072





Enterprise Content Management mit Alfresco

# An der frischen Luft

Andreas Popper

Ein Enterprise-Content-Management-System zu entwickeln stellt eine Herausforderung dar. Im Juli 2007 ist das als Open Source vorliegende Alfresco mit der Version 2.0 „angetreten“ und hat das Potenzial, gegenüber proprietären Produkten zu bestehen.

Momentan sind in Deutschland über hundert Anbieter für ECM-Produkte am Markt [b]. Für den Unternehmenseinsatz waren bisher nur proprietäre Angebote geeignet, die durchweg kostspielig sind. Mit Alfresco (engl.: draußen, im Freien) erreicht Open Source diesen Bereich, parallel als Community und Enterprise-Variante. Sie sind Code-identisch, für die Community-Version steht aber kein Support zur Verfügung. Stattdessen gibt es eine ausführliche Dokumentation in einem eigenen Wiki [c] und mehreren Foren [d].

2005 ging Alfresco aus dem Java Web Development and Portal Team von Documentum (inzwischen bei EMC) hervor. Die Community Edition erschien im Dezember 2007 in der aktuellen Release 2.9.0B (B steht für zweite Auslieferung, nicht für Beta), Code-identisch mit der Enterprise Edition 2.1.1, von der jetzt 2.2 vorliegt. Noch in diesem Jahr soll die Version 3.0 folgen.

## Architektur und Schnittstellen

Alfresco verwendet als Open Source erhältliche und auf Java aufsetzende Werkzeuge. Die Entwickler streben jedoch an, das System für andere Sprachen zu öffnen. Bei der Auswahl der Komponenten haben sie vor allem auf Qualität geachtet und sich vorzugsweise bei Standards, Referenz-Anwendungen für Standards oder De-facto-Standards wie Java, Apache und MySQL bedient (siehe Abb. 1).

Eine ausführliche Darstellung der Architektur findet sich in der zentralen Dokumentationsquelle der Community Edition. Prinzipiell entspricht sie einer für Webarchitekturen üblichen: Datenbank-Backend, Application Server für Verarbeitung und Auslieferung sowie Browser als Frontend. Das Besondere ist die Trennung in zwei Schichten innerhalb des Application Server: Das Repository verwaltet die Daten – Speicherung, Versionierung, Suche und Transformation zwischen Datenformaten –, während in der Schicht darüber die Daten in unterschiedlichen Darstellungen eingefügt werden: Dokumenten-Management, Vorgangsbearbeitung (Records Management) oder Web Content Management.

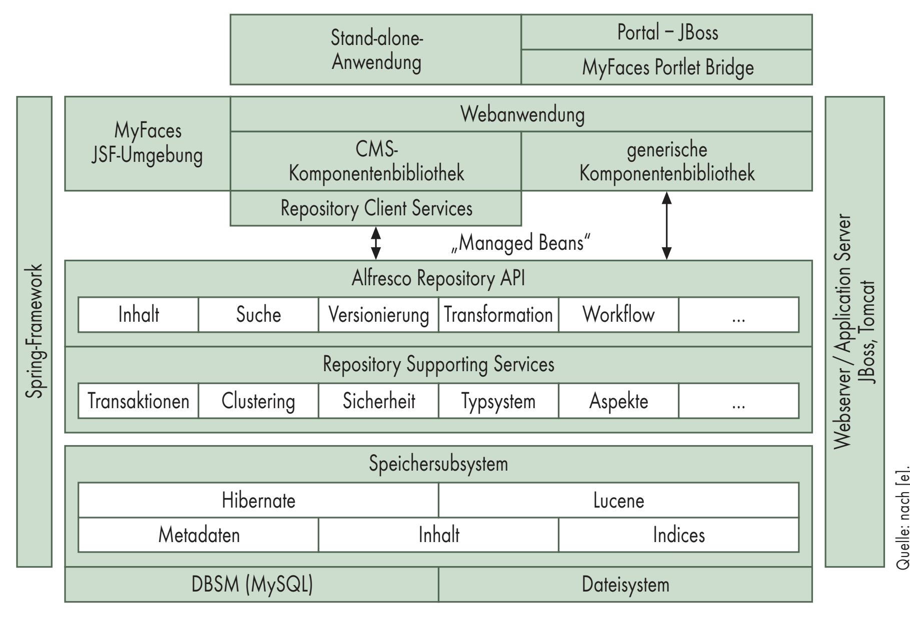
Repository und Applikationen kommunizieren über Schnittstellen, sodass sie unabhängig voneinander ausgebaut werden können. Hier zeigt sich das konsequent modulare Design von Alfresco, das es erleichtert, Erweiterungen zu schreiben und einzubinden. Obwohl die Major Release zu 2.0 erst vor einem guten halben Jahr herauskam, existieren schon einige von Drittanbietern geschriebene Erweiterungen [f].

## Anmerkungen zum Installieren

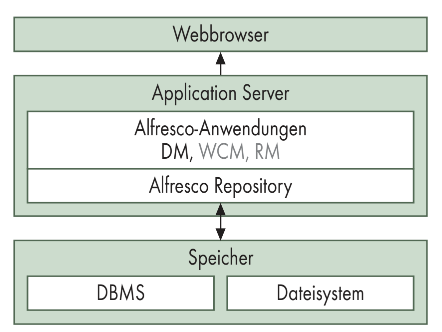
Alle zur Community Edition gehörenden Softwarepakete finden sich bei Sourceforge [g]. Für Linux und Windows gibt es ausführbare Programme, mit denen eine Grundinstallation in wenigen Minuten erledigt ist. Wer Alfresco mit MySQL installieren will, findet dafür ein fertig geschnürtes Paket bei Bitnami (siehe den *iX*-Link am Ende des Artikels), ebenfalls für Windows und Linux. Allerdings ist dort nur das englische Sprachpaket enthalten, andere Sprachen muss man nachrüsten.

Alfresco bringt von Haus aus als Datenbank-Engine HSQLDB mit. Zum Ausprobieren reicht das, für die Produktion muss man aber MySQL, Oracle, PostgreSQL, Microsofts SQL-Server oder Sybase anbinden.

Ursprünglich sollte Alfresco keine anderen Clients als Browser erzeugen und bedienen. Es gibt allerdings eine Schnittstelle zu Microsofts Common Internet File System (CIFS), mit dem




**So sehen die Entwickler Gavin Cornwell und Kevin Roast die Komponenten Alfrescos: von JBoss über Tomcat und Spring bis zu MySQL (Abb. 1).**




**Einfaches Diagramm von Alfresco – nach der Dokumentation (Abb. 2)**

sich bequem Ordner als Netzlaufwerke mounten lassen. Dort steht ein Check-in/Check-out zur Verfügung, und damit können beliebige Anwendungen ihre Dateien direkt in Alfresco ablegen.

Es hat sich aber gezeigt, dass viele Benutzer ihre Dateien ausschließlich in Microsofts Office-Suite verwalten. Deshalb hat Alfresco eine Erweiterung für dieses Produkt gebaut, die sich als zusätzliche Schaltfläche in die Symbolleisten von Microsofts Word einfügt.

Alfrescos Office-Plug-in liegt ebenfalls bei Sourceforge vor. Man kann seine Anmeldedaten speichern lassen und hat dann aus Office heraus unmittelbaren Zugriff auf das ECM (siehe Abb. 3). Der Client ist praktisch eine verkleinerte Ausgabe des Webclients. Anwender können nicht nur Dokumente ein- und auschecken sowie hoch- und herunterladen; zum Erzeugen neuer Ordner brauchen sie die Ansicht nicht zu wechseln, die Suchfunktion ist unmittelbar erreichbar, einen Workflow kann man anlegen oder das Office-Dokument in ein PDF verwandeln. Außerdem steht der Webclient über einen Klick jederzeit zur Verfügung.

Für Bürokräfte, die tagtäglich mit dem ECMS arbeiten müssen, bedeutet das eine große Erleichterung, was sicherlich ein starkes Akzeptanz-Argument liefert. Leider gibt es nichts Vergleichbares für Openoffice, was an dessen ganz anderer Programmstruktur liegt. Über den CIFS-Server und Netzlaufwerke lassen sich Openoffice und Alfresco aber recht komfortabel gemeinsam nutzen.

## ECMS als Netzlaufwerk einbinden

Eine Besonderheit: Anders als in den Anleitungen zum Abbilden von Netzlaufwerken sollte man keinen Unterordner innerhalb von Alfresco als Netzlaufwerk ansprechen. Denn in diesem Fall funktioniert das Ein- und Auschecken im Explorer nicht. Besser ist es, das gesamte ECMS als Netzlaufwerk einzubinden, etwa in der Form: \\<*Computername*>*A\alfresco*. Ebenfalls anders als in der offiziellen Dokumentation steht ab Version 2.1 zwischen „Computername" und „A" kein Unterstrich mehr.

Für das Check-out und Check-in gibt es einen ganz einfachen Mechanismus. In jedem Unterordner des Netzlaufwerks finden sich zwei Dateien: *_CheckInOut.exe* und *_ShowDetails.exe*. Wenn man ein Dokument per Drag & Drop auf Erstere zieht, checkt Alfresco sie aus und legt eine Arbeitskopie an. Zum Einchecken zieht man die Arbeitskopie auf die Datei, die Arbeitskopie verschwindet und das Dokument ist mit seinen Änderungen eingecheckt sowie versioniert, wenn denn Versionierung aktiviert ist. Außerdem findet sich in jedem Ordner ein Link zum Webclient, der dort genau den Ordner öffnet.

Während des Hochladens indiziert das System die betreffenden Dokumente sofort, sodass sie unmittelbar danach mit der Volltextsuche auffindbar sind. Dazu muss man aber einmal das zusammen mit Alfresco installierte Openoffice gestartet haben.

Alfresco verwendet die vielfältigen Fileformatkonversionen von Openoffice intern, um beispielsweise Microsoft-Office-Dokumente indizieren zu können.

## Hochgezählte Versionsnummer

Die Versionierung muss der Anwender entweder für jedes einzelne Dokument von Hand aktivieren, oder er erstellt über den Regel-Generator eine diesbezügliche Regel. Die Versionierungsfunktion für ganze Ordnerstrukturen liegt allerdings etwas versteckt, weil sie zum umfangreichen und differenzierten Regelgenerator gehört. Im Ergebnis weist Alfresco jedem danach hochgeladenen Dokument automatisch die Version 1.0 zu und zählt sie bei jedem Check-out und Check-in weiter hoch. Unprotokollierte Änderungen an Dokumenten gibt es ab diesem Zeitpunkt nicht mehr.

Um zu verhindern, dass mehrere Benutzer gleichzeitig an einem Dokument arbeiten, enthalten Dokumenten-Management-Systeme einen Check-in/Check-out-Mechanismus. Beim Hochladen der geänderten Version wird ein Einchecken verlangt und das alte Dokument ersetzt. Ist Versionierung aktiviert, erhält das neue Dokument eine höhere Nummer, sodass das ältere weiterhin über die Versionshistorie existiert.

Zur Formattransformation nutzt Alfresco Openoffice. Über den Regelgenerator kann so beispielsweise der Anwender festlegen, dass Alfresco von einem hochgeladenen MS-Word-Dokument sofort eine Kopie im PDF-Format anfertigt und in einem anderen Ordner speichert. Etwa, wenn intern noch bear-

### iX-TRACT

- Alfresco ist das erste ernstzunehmende Enterprise-Content-Management-System im Open-Source-Bereich.
- Seine Stärken hat es vor allem in der Vorgangsbearbeitung und Archivierung.
- Die Einarbeitung ist wegen der großen Komplexität recht aufwendig.

## Software-Evaluierung fürs ECM

Enterprise Content Management ist zunächst ein Konzept. Es soll alle unternehmensrelevanten Daten zusammenführen, um sie leicht erreichbar, durchsuchbar und sicher archivierbar zu machen sowie Redundanz und Inkongruenz zu vermeiden. Alle auf dem Markt befindliche Software deckt nur Teilbereiche davon ab.

Wo immer Entscheider vor der Aufgabe stehen, Software für den Umgang mit Unternehmensdaten anzuschaffen, ist zuerst zu klären: Soll es die viel zitierte eierlegende Wollmilchsau, die Suite oder das Mash sein, wo fast alle Funktionen „out of the box“ kommen? Die Alternative ist, eine Best-of-Breed-Softwaresammlung zusammenzustellen – aus weitgehend getrennt voneinander operierenden Spezialisten, die auf ihrem Gebiet erprobt und führend sind.

Beides hat Vor- und Nachteile. ECM-Systeme sind ein einheitlicher Ansatz und damit für alle, die damit arbeiten sollen, als Standard einzuführen. Hinter den Produkten stehen leistungsfähige Unternehmen. Nach Einführung der Suite braucht man sich nur an einen Ansprechpartner zu wenden, gleichgültig, in welchem Bereich der Software oder ihrer Anpassung ans Unternehmen Schwierigkeiten auftreten. Und die Angestellten müssen sich nur eine zusätzliche Software erarbeiten, die sich günstigenfalls gut in ihre bisherige Arbeitsumgebung einfügt.

Dem steht die heterogene Landschaft des Best-of-Breed gegenüber, meist historisch gewachsen und in vielen ihrer Bestandteile im Unternehmen eingeführt. Einerseits dürfte man in solchen Fällen auf weniger Widerstand bei dem Vorhaben stoßen, diese Sammlung zu einer vollständigen ECM-Lösung aufzubohren; andererseits tendieren Angestellte zum „Weiter so“. Und zur Vermeidung von Dateninkongruenzen, beispielsweise zwischen Warenwirtschaft und Dokumentenmanagement, sind gezielte Anstrengungen erforderlich.

### Begriffsbestimmung und Bestandteile

Diese Entscheidung muss also vorab getroffen werden. Aber davon unabhängig gilt es zu klären, welche Kriterien die gewählte Software erfüllen muss, um dem Konzept Enterprise Content Management gerecht zu werden. Immerhin handelt es sich um eine unternehmenskritische Funk-

### Fragen zur ECMS-Evaluation

Für die Einschätzung eines ECMS kann die folgende Fragenliste als Richtschnur dienen.

– Lässt sich das System mit überschaubarem Aufwand installieren?

– Gibt es eine ausreichende Dokumentation?

– Ist ein Support (in der Enterprise Version) gewährleistet?

– Wie groß und rührig ist die Community der Entwickler?

– Existieren Erweiterungen von Drittanbietern? Wie umfassend sind die?

– Ist die Performance ausreichend? Skaliert das System bei größeren Anforderungen ausreichend?

– Lassen sich wirklich alle Arten, Typen und Verwendungszwecke von Dokumenten und Inhalten im Unternehmen im ECM zusammenführen?

Ergänzungen nach Kampffmeyer:

– Sind alle Komponenten mit allen anderen kompatibel?

– Ist das ECM-System modular und komponentenweise erweiterbar?

– Werden gemeinsame Administrationskomponenten genutzt (Sicherheit, Zugriff, Metadaten, Speicherorte et cetera)?

– Werden alle Informationen durch alle Komponenten einheitlich genutzt?

– Sind alle Komponenten auf allen Plattformen des ECM-Systems lauffähig?

– Gibt es einheitliche Clients für das gesamte ECM-System?

– Sind die Komponenten als Bestandteile des ECM-Systems ausgerichtet?

– Existieren für alle Komponenten gemeinsame Weiterentwicklungspläne?

– Ist das ECM-System vollständig? Decken die Komponenten alle nötigen Funktionen ab?

– Werden Standards eingehalten, um Komponenten von Drittanbietern einbinden zu können?

– Existiert ein konsistentes Vertriebs- und Marketing-Konzept?

#### Erfassung von Dokumenten

– Lassen sich Dokumente aus allgemein verbreiteten und schon vorher benutzten Anwendungen wie E-Mail-Servern oder ERP-Systemen nutzen?

– Kann das System Dokumenten-Scans erfassen und gegebenenfalls weiterverarbeiten (OCR)?

– Wie werden Dokumenten-Scans in das ECM-System einsortiert?

– Können schriftliche Formulare erfasst und weiterverarbeitet beziehungsweise elektronische Formulare automatisch weiterverarbeitet werden?

– Können angelieferte Dateien anhand von Strukturinformationen indiziert und an eine dynamische Ablage oder ein Archiv übergeben werden?

– Können elektronische Dokumente indiziert werden?

– Gibt es Input-Designs (Eigenschaftsprofile, Erfassungsmasken)?

– Ist eine Kategorisierung beziehungsweise Klassifikation aufgrund im Dokument enthaltener Informationen möglich?

#### Verwaltung, Bearbeitung und Nutzung

Allgemein:

– Existiert eine zentrale Datenbank für das Verwalten und Wiederauffinden von Informationen?

– Gibt es eine zentrale Benutzerverwaltung für alle ECM-Komponenten mit differenzierter Rechtevergabe?

Stichpunkte zum Dokumentenmanagement:

– Mechanismus zur Kontrolle der Konsistenz? (Check-in/Check-out oder Merge à la Subversion)

– Versionsmanagement?

– Suche mit Volltextsuche in üblichen Dokumentformaten (.doc, .pdf et cetera)?

– Strukturierung von Dokumenten, Zusammenfassung zu virtuellen Akten, Verzeichnissen und Übersichten

– Benutzerfreundliche Navigation (TreeView à la Explorer)

– Existiert eine Schnittstelle zu Office-Anwendungen?

Fragen zur Zusammenarbeit (Kollaboration, Groupware:)

– Können Mitarbeiter gemeinsam auf Informationen zugreifen und sie kontrolliert (Versionierung) bearbeiten?

– Können Mitarbeiter Informationsbasen gemeinsam nutzen?

– Existieren Verwaltungskomponenten für Ideensammlungen, Terminpläne, Projektmanagement et cetera?

– Existieren Kommunikationsanwendungen (Video-Conferencing, Chat)?

– Werden Informationen aus anderen Anwendungen integriert (Statusberichte, ERP)?

tion, gravierende Fehler darin können schnell das Aus bedeuten.

Vom internationalen Dachverband AIIM – The Enterprise Content Management Association [j], der seit über 60 Jahren in diesem Bereich aktiv ist, stammt die Definition des ECM, wie sie der Wikipedia-Artikel nach Ulrich Kampffmeyer verwendet. Danach setzt sich ein solches System aus den fünf Hauptkomponenten Erfassung, Verwaltung, Speicherung, Bewahrung und Ausgabe zusammen. Die Verwaltung besteht wiederum aus den fünf Unterkomponenten Dokumentenmanagement, Zusammenarbeit unterstützende Systeme, Web Content Management, Archiv- und Ablageverwaltungssysteme inklusive Langzeitarchivierung sowie Vorgangsbearbeitung.

Eine weitergehende Beschreibung der Vorgangsbearbeitung mit Ausrichtung auf das Verwaltungshandeln findet sich im DOMEA-Konzept der KBSt [i]. Nicht alle dort aufgeführten Anforderungen an ein „Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang“ finden sich in den ECM-Anforderungen wieder. Wenn eine Organisation in diesem Bereich hohe Anforderungen hat, lohnt es sich ganz sicher, diese Quellen bei der Evaluierung zu konsultieren.

Aus der Begriffsbestimmung zum ECM lassen sich Fragen ableiten, die man zur Evaluation an die ins Auge gefasste Software stellen kann – unabhängig davon, ob man sich für eine Suite oder ein Best-of-Breed entschieden hat. Es wurde darauf verzichtet, die im Kasten zusammengestellten Fragen zu gewichten: Einstufungen wie „Muss“, „Kann“ oder „Wäre nett“ sind von Organisation zu Organisation zu verschieden.

## Fazit

Ein wie auch immer zusammengestelltes ECM-System, das alle Fragen befriedigend beantworten kann, gibt es derzeit nicht. Gerade in der Vorgangsbearbeitung und der Langzeitarchivierung klaffen noch größere Lücken, die auch den E-Government-Experten noch Kopfschmerzen bereiten. Aber anhand der Fragen lässt sich recht gut klären, was die ins Auge gefasste Software leisten kann, was nicht und wo sie ergänzt werden muss.

Web Content Management:

– Ist die Erstellung oder Aufbereitung von Informationen in einem kontrollierten Erstellungs- und Veröffentlichungsprozess (Workflow, Genehmigungswege) vorgesehen?

– Können Informationen für die Webpräsenz bereitgestellt und verwaltet werden?

– Lassen sich unterschiedliche Anzeigeformate automatisch konvertieren (.doc zu PDF, XML zu HTML, PDF et cetera)?

– Ist die Einrichtung personalisierter Anzeigen möglich?

– Existiert auch für die Webinformationen eine Versionierung?

– Können Zugriffe auf öffentliche und nicht öffentliche Informationen sicher getrennt werden (dedizierte Rechtevergabe)?

– Können die vorhandenen Daten für die Browser-Darstellung visualisiert werden (HTML, XML)?

Ablage- und Archivverwaltung:

– Entspricht das Records Management (RM) der ISO 15489?

– Ist das Records Management speicherunabhängig?

– Lassen sich Aktenpläne und andere strukturierte Verzeichnisse zur Ablage von Informationen abbilden?

– Existiert eine eindeutige Identifizierung und Klassifizierung von Informationen?

– Werden Aufbewahrungs- und Vernichtungsfristen verwaltet?

– Ist die Originalität von Dokumenten gewährleistet?

– Werden standardisierte Metadaten (Dublin Core) zur Identifizierung und Beschreibung von Dokumenten vergeben?

### Bearbeitung von Vorgängen

– Wie fest sind Workflows vorgegeben?

– Können Anwender Workflows ad hoc selbst festlegen?

– Können Ablauf- und Aufbauorganisationsstrukturen im Workflow abgebildet werden?

– Werden zusammenhängende Informationen (etwa ganze Akten) empfangen, verwaltet, visualisiert und weitergeleitet?

– Sind Bearbeitungswerkzeuge eingebunden (Microsofts Office et cetera)?

– Ist die parallele und sequenzielle Bearbeitung von Vorgängen einschließlich Mitzeichnung der Bearbeitung möglich?

– Existieren Design-Werkzeuge zur Gestaltung und Anzeige von Prozessen (Geschäftsprozessmodellierung)?

– Gibt es Regelungen zu Wiedervorlage, Fristen, Delegation und dergleichen?

– Können Bearbeitungsstände, Laufwege und Ergebnisse kontrolliert und dokumentiert werden?

### Ablage (Store) und Archiv (Preserve)

– Welche Speicherorte (Dateisystem, Content Management System, Datenbank, Data Warehouse) stehen zur Verfügung? Wie sind die Aufgaben (Speichern, Indizieren) verteilt?

– Sind die Suche nach und das Wiederfinden von Informationen gewährleistet?

– Werden Offline-Speicher verwaltet?

– Welche Speichertechniken kann das ECM-System ansprechen?

– Existiert eine geregelte Übergabe von Informationen an das Archiv?

– Ist die stabile, statische und unveränderbare Aufbewahrung und Sicherung von Informationen auf lange Zeit gewährleistet?

– Welche Speichermedien können verwendet (und wiedergefunden) werden?

– Wie ist die endgültige Löschung nicht mehr benötigter Informationen (Kassation) geregelt?

– Existieren Migrationsstrategien für Hard- und Software (Continuous Migration)?

### Liefern, Bereitstellen, Ausgeben

– Existieren Layout-Werkzeuge zur Gestaltung und Formatierung der Ausgabe für unterschiedliche Medien?

– Wie erfolgt das Publishing von Dokumenten?

– Ist der verlustfreie, kontrollierte und nachvollziehbare Ablauf von Transformationen gewährleistet?

– Welche Sicherheitstechniken kommen zur Anwendung (elektronische Signaturen, Digital Rights Management)?

– Können abgesicherte Verbindungen aufgebaut werden (Virtual Private Networks, Secure Shell)?

– Wo werden die Inhalte zur Verfügung gestellt (Internet, Extranet, Portale, Datenträger, Medien, Papier)?

beitete Dokumente in der jeweiligen Version der Öffentlichkeit zugänglich sein sollen: Gesetzestexte, Normen und dergleichen.

Bilder lassen sich beim Laden ebenfalls zwischen verschiedenen üblichen Formaten transformieren. Steht allerdings für ein zu ladendes Format keine Transformation zur Verfügung, scheitert der Vorgang. Mit der Anwendung solcher Regeln sollte man daher vorsichtig sein.

Über den Regel-Generator können Anwender beliebig komplexe Workflows erstellen. Mehrere Personen können Dokumente zur Bearbeitung erhalten; andere können zeichnen und mitzeichnen, sodass ein Dokument erst veröffentlicht wird, wenn alle eingetragenen Personen es gesehen und genehmigt haben. Wollen sie das nicht, können sie es mit einer Bemerkung, was daran auszusetzen ist, zurückschicken.

Jeder Benutzer hat ein persönliches sogenanntes Dashboard. Auf dem erscheinen die ihm zugeordneten Aufgaben inklusive der Dokumente, die er bearbeiten oder genehmigen soll.

Die Einrichtung dieser Workflows ist ziemlich komplex, weil der Regelgenerator ein mächtiges Werkzeug mit vielen Wahlmöglichkeiten ist. Alle Vorgänge einer Verwaltung auf die Ordnerstruktur abzubilden, kann etliche Arbeitsstunden verbrauchen; wer das hingegen erledigt, dem steht ein komfortabler Automatismus zur Verfügung.

## Erweiterungsmodul Vorgangsbearbeitung

Für Alfresco gibt es ein Records Management als Erweiterungsmodul. Das ergänzt die so schon beachtlichen Fähigkeiten des Dokumenten-Managements um eine Vorgangsbearbeitung. Alfresco bietet zum Installieren einen standardisierten Weg, bei dem es Module in das *.war*-Archiv kopiert und dort auspackt. Das Records-Management-Modul findet sich ebenfalls auf der Sourceforge-Seite. Es einzuspielen erfolgt über die Kommandozeile mit dem Modul-Manager.

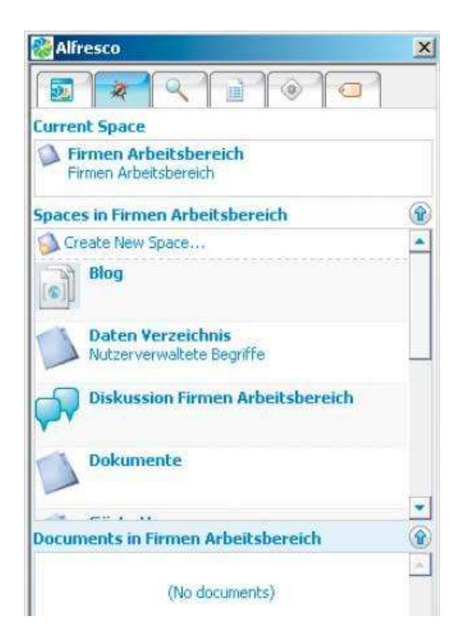
Danach muss ein Admin den *alfresco*-Ordner im *tomcat\webapps*-Verzeichnis löschen, damit beim nächsten Serverstart die Änderungen wirksam werden können. Das Modul-Management legt beim Einrichten automatisch eine Backup-Datei von *alfresco.war* im *webapps*-Verzeichnis an, mit der man den ursprünglichen Zustand wiederherstellen kann.

Nach dem Start taucht im Basisverzeichnis ein zusätzlicher Ordner namens Records Space auf. Er enthält eine Beispielumgebung für ein Vorgangsbearbeitungssystem, basierend auf der Norm DOD 5015-2 des amerikanischen Verteidigungsministeriums, die Designkriterien für elektronische Vorgangsbearbeitungen beschreibt. Leider haben die Entwickler an dieser Stelle nicht ISO 15489 [h] verwendet, bei ihrer Entstehung 2001 als Durchbruch bei der Internationalisierung von Schriftgutverwaltung, Vorgangsbearbeitung und Archivierung gefeiert.

## Aktenplan im Verwaltungsenglisch

Um einen eigenen Aktenplan zu erstellen, öffnet man den Assistenten für den erweiterten Arbeitsbereich. Mit der Installation des Records Managements steht dort als zusätzlicher Arbeitsbereichstyp ein File Plan zur Verfügung. Er verfügt über eine ganze Reihe mehr Eigenschaften als im normalen Dokumentenmanagement. So verlangt er zwingend einen Record Category Identifier (Aktenzeichen). Jedes in diesen Ordner hochgeladene Dokument wird automatisch durchnummeriert; damit sind alle einem Aktenzeichen zugehörigen Dokumente eindeutig identifizierbar. Außerdem aktiviert Alfresco automatisch die Versionierung.

Zur Abbildung vorhandener Geschäftsvorgänge muss man die Eigenschaften des Aktenplanes ändern. Dabei fällt eine durchgehend vorhandene




**Viele ECM-Funktionen sind direkt über das Office-Plug-in erreichbar (Abb. 3).**

Schwäche von Alfresco besonders unangenehm auf: die unvollständige Eindeutschung. Eigenschaften des Aktenplans erscheinen, bis auf den Kopfteil, vollständig auf Englisch, und zwar Verwaltungsenglisch, was schnell sonst profunde Fremdsprachenkenntnisse überfordert.

In den Eigenschaften lässt sich jetzt festlegen, wie mit der Akte zu verfahren ist: mit der Gültigkeitsdauer, was mit ihr nach deren Ablauf passiert, etwa Wiedervorlagefristen et cetera. Über den Regelgenerator können Verwaltungsakte bestimmt und ein Workflow festgelegt werden.

Im Verein mit dem Regelgenerator ist das Records Management ein mäch-




**Vielfältige Aktionsmöglichkeiten im Regelgenerator (Abb. 4)**

tiges, vielseitig einsetzbares Werkzeug, mit dem sich die meisten Akte des Verwaltungshandelns abbilden lassen.

## Web Content Management inbegriffen

Über eine Sandbox kann man die Website der Organisation verwalten. Die Website wird komplett in einer eigenen Umgebung mit einem virtuellen Webserver erzeugt, wobei beliebige Inhalte als Material dienen können. Für die Website können Administratoren ebenfalls Workflows definieren, beispielsweise für serielle oder parallele Genehmigung, die Absegnung durch eine einzelne oder mehrere Kontrollinstanzen.

Weil Alfresco auch beim Web Content Management (WCM) konsequent XML verwendet, können die Seiten für unterschiedliche Darstellungen eingerichtet werden, beispielsweise HTML, einfachen Text und PDF. Weitere Output-Formate stehen zur Verfügung.

Per Workflow landen die von verschiedenen Benutzern erzeugten Seiten in einer Staging Sandbox, sozusagen auf der Bühne. Davon fertigt Alfresco einen Snapshot an und versioniert ihn. Und erst wenn der Snapshot vorliegt, kopiert das WCMS die fertige Webseite auf den eigentlichen Webserver.

In seiner Struktur ist das WCMS recht komplex. Glücklicherweise gibt es ein ausführliches Tutorial. So weit die Theorie. In der Praxis erweist sich das WCM als noch fehlerhaft. Und wenn man schließlich die erzeugte Webseite live erleben will und sie nach Anweisung auf eine andere Serverinstanz von *localhost* mit dem Port 50500 exportiert (Deployment), bekommt man eine leere Seite vorgesetzt, ohne Fehlermeldung. Hier hat die Recherche in einschlägigen Alfresco-Foren noch keine Lösung ergeben. Nach den vielen Hilferufen im Forum zu urteilen, scheint das WCM derzeit beim Deployment aufzugeben. Man hat nicht den Eindruck, dass es jemand in der Version 2.9.0B zum Laufen gebracht hat.

Wer die Fragen zum Evaluieren (siehe den Kasten „Software-Evaluierung fürs ECM“) mit Alfresco abarbeitet, dürfte seine prinzipielle Eignung als ECM-Suite feststellen. Die meisten dort verlangten Funktionen und Eigenschaften sind vorhanden. Es schwächelt bei der Zusammenarbeit: Ideensammlungen, Schwarzes Brett, Terminpläne – alles Fehlanzeige. Es gibt ein Wiki-Modul, aber das funktioniert seit Version 2.1 nicht mehr.

Als großes Plus kann das Records Management gelten. Hier lassen sich alle Verwaltungsfunktionen darstellen, die weit über die eines Dokumenten-Management hinausgehen. Regelgenerator und Workflow erweitern es noch und lassen wohl nicht mehr viele Wünsche offen. Das Gesagte bezieht sich auf die Commmunity-Version. Kommerzielle Anbieter haben da durchaus mehr zu bieten, beispielsweise komplette Archiv-Systeme oder Anbindungen an ERP-Software. Das Lizenzmodell von Alfresco sieht aber nicht vor, dass zertifizierte Partner solche Erweiterungen der Community zugänglich machen dürfen.

## Fazit

Zweierlei vermisst man schmerzlich. Zunächst ein Administrationstool, das die Konfiguration erleichtert, vor allem nach der Installation zusätzlicher Module. In Dutzenden von Konfigurationsdateien an verschiedenen Orten von Hand die nötigen Eintragungen vornehmen zu müssen, ist unproduktiv und fehleranfällig.

Zudem fehlt ein Instrument zur Nachverfolgung und Konfiguration der Vorgangsbearbeitung. Wenn in einem ganzen Aktenplan über mehrere Hundert Ordner verschiedene Workflows und Regeln eingerichtet werden, geht irgendwann der Überblick verloren.

Nicht zu übersehen, dass es sich um Work in Progress handelt: Sei es beim Installieren von Modulen und Konfigurieren von Funktionen, sei es die Einbindung ins CIFS, ans Active Directory über LDAP oder die Transformation von Dateiformaten, man kommt nicht umhin, das Wiki und die Foren nach den benötigten Tricks und Workarounds zu befragen. Und manche Dinge funktionieren selbst nach mehreren Anläufen nicht.

Auf der anderen Seite verfügt Alfresco über ein gewaltiges Potenzial und ist mit seinem modularen Aufbau offen für Erweiterungen. Für die Open-Source-Community ein bedeutender Neuzugang, wo Enterprise Content Management bislang nicht gerade üppig vertreten war. Es bleibt zu hoffen, dass die im Spätsommer erwartete Release 3.0 vor allem die bestehenden Schwächen reduziert. (hb)

ANDREAS POPPER

ist Diplom-Agrar-Ingenieur und arbeitet freiberuflich im Bereich Dokumentenmanagement und Langzeitarchivierung.





### Onlinequellen

[a] ECM-Definition
www.jdk.de/de/cms/ecm-enterprise-content-management/was-ist-ecm/ecm-ist-ein-konzept.html

[b] ECM-Anbieter
www.contentmanager.de/itguide/marktuebersicht_produkte_cms_enterprise.html

[c] Alfresco-Homepage
wiki.alfresco.com/wiki/Main_Page

[d] Alfresco-Forum
forums.alfresco.com/

[e] Alfresco aus Entwicklersicht
www.jsfcentral.com/articles/trenches_5.html

[f] Alfrescos Entwickler-Community
forge.alfresco.com/

[g] Alfresco-Download
sourceforge.net/projects/alfresco/

[h] Verwaltungsnorm ISO 15489
www.coi.de/download/ISO_DIN_15489.pdf

[i] DOMEA Homepage
www.kbst.bund.de/nn_836802/Content/Standards/Domea__Konzept/domea__node.html__nnn=true

[j] ECM-Definition des internationalen Dachverbandes AIIM
www.aiim.org

### iX-Wertung

⊕ Open-Source- und Enterprise-Edition Code-identisch

⊕ plattformunabhängig

⊕ umfangreiche ECM-Funktionen

⊕ rührige Community

⊖ mangelhafte Nationalisierung

⊖ umständliche Konfiguration

⊖ einige Fehlfunktionen

⊖ Dokumentation nicht immer gut

### Daten und Preise

Alfresco,
Enterprise-Content-Management-System

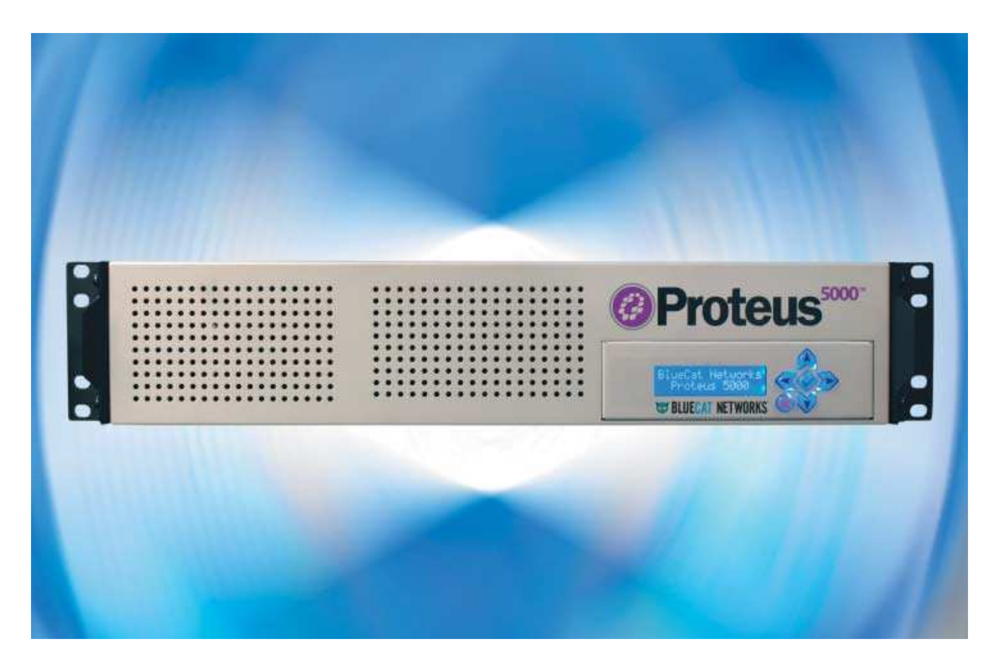
**Community Edition:** 2.9.0B (kostenlos)

**Download:** sourceforge.netprojects/alfresco/

**Enterprise Edition:** 2.1.1

**Bezug:** www.alfresco.com

**Preis:** 16 125 Euro pro Jahr und CPU




IP-Adressmanagement-System im Praxistest

# Nummernvergabe

**Manuel Schmitt**

Das Verwalten und Verteilen von IP-Adressbereichen erweist sich in vielen Unternehmen als zeitaufwendige Herausforderung für die IT-Abteilung und führt nicht selten zu einem Flickenteppich. Ein geeignetes IP-Adressmanagement kann Zeit und Geld sparen.

Viele Unternehmen fangen klein an, mit einer Handvoll Workstations sowie je einem Switch, Router und netzwerkfähigen Drucker. Die Definition der Netztopologie befindet sich meist an genau zwei Stellen: In den Geräten selbst und im Kopf des Administrators. Im Laufe der Zeit kommen Geräte hinzu, und gelegentlich steckt irgendjemand behelfsmäßig etwas um oder vergibt die eine oder andere neue Adresse.

Sobald ein neuer Administrator hinzukommt oder den alten ersetzt, ist das Suchen und Raten oft die erste Amtshandlung vor dem Beheben von Fehlern oder dem Erweitern des bestehenden Netzes. Administratoren, die vorsorgen oder die Arbeit ihres Vorgängers ordentlicher gestalten möchten, beginnen mit einer Netzdokumentation analog zur tatsächlichen Situation (statisch eingerichtete oder per DHCP vergebene IP-Adressen, DHCP- und DNS-Server). Meist kommen dafür gewöhnliche Textverarbeitungs- oder Tabellenkalkulations-Dokumente oder auch Wikis zur Anwendung.

Sobald die Netze wachsen, mehrere Standorte umfassen oder gar mehrere Administratoren am Werkeln sind, stoßen auch solche Provisorien schnell an ihre Grenzen. Zunächst gibt es ein prinzipielles Manko: Es fehlt ein direkter Zusammenhang zwischen der Technik, also etwa den DNS- und DHCP-Servern, und der Dokumentation. Damit verbunden gibt es keine Form der Zugriffsbeschränkung. Häufig fehlt bei solchen Dokumentationsverfahren eine Historie, und eine produktive Zusammenarbeit ist praktisch unmöglich.

Erleichterung für den Administratorenalltag verspricht ein IP-Adressmanagement-System wie die Appliances der Proteus-/Adonis-Reihe von Bluecat Networks. Das Konzept dahinter ist so simpel wie logisch. Eine Verwaltungseinheit (Proteus) mit Überblick über das gesamte Unternehmensnetz steuert die DHCP- und DNS-Server (Adonis). Letztere können über mehrere Standorte verteilt sein, auch über Kontinente hinweg.

## Adressenverteilung automatisiert

Der oder die Administratoren arbeiten in der Regel mit der Weboberfläche des Proteus-Servers, der den oder die angeschlossenen Adonis-Server selbstständig steuert und überwacht. Gerade im Hinblick auf Unternehmen mit mehreren Niederlassungen ein einleuchtendes Design, wenn an jedem Standort DHCP-/DNS-Server stehen sollen.

Ein solches Konzept klingt auf den ersten Blick banal und könnte programmiererfahrene Administratoren dazu herausfordern, einige Stunden mit einer Skriptsprache in ein eigenes Projekt zu investieren. Doch die beiden Produkte bieten einen immensen Funktionsumfang – praktisch alles, was der geplagte Admin zum Bewältigen seiner Aufgaben benötigt, und damit wenig Anlass, das Rad neu zu erfinden.

Selbst Neulingen fällt es nicht schwer, beide Produkte in Betrieb zu nehmen. Wer mit unixoiden Betriebssystemen vertraut ist, fühlt sich angesichts der schlicht gehaltenen Netzkonfiguration via Konsole sofort wohl. Anschließend sind Proteus und Adonis zum Einsatz bereit, alles Weitere erfolgt direkt über die Proteus-Weboberfläche.

## Schlichte Oberfläche schafft Überblick

Wer mit einem komplizierten Web-GUI rechnet, zu dessen Verständnis Handbücher oder gar eine Schulung nötig sind, liegt falsch. Trotz ellenlanger Feature-Liste ist der erste Blick auf die Administrationsoberfläche eher ernüchternd als erschlagend.

Nach dem Einrichten kann Proteus bestehende Daten – sofern vorhanden – übernehmen, etwa MAC- und IP-Adressen in CSV-Dateien. Wer die Datenbank-Felder anpassen oder eigene Angaben hinzufügen möchte (zum Beispiel Standort-Angaben zu MAC-Adressen), sollte etwas Programmiererfahrung mitbringen, denn dies erfolgt



**Bluecat Networks rüstet seinen Proteus mit redundanten Netzteilen aus und erneuert die Hardware im Dreijahresturnus (Abb. 1).**

per XML-Datenaustausch. Die laufende Administration über Proteus umfasst vor allem die Verwaltung von MAC- und IP-Adressen sowie des DNS.

Alle angeschlossenen Netzwerkgeräte sind auf Basis ihrer MAC-Adressen erfasst. Idealerweise legt man hier alle im gesamten Netzwerk befindlichen Geräte, also Workstations, Server, Netzwerkgeräte et cetera an. Neben der MAC-Adresse kann standardmäßig jedes „Gerät“ einen selbstdefinierten Namen sowie bei Bedarf eine statische IP-Adresse erhalten.

Wünschenswert wäre es, dass Proteus jede MAC-Adresse beim Anlegen automatisch um den Namen des Hardwareherstellers ergänzt; die Präfix-Zuordnungen sind schließlich frei zugänglich. Gerade bei der Migration eines bestehenden großen Netzwerks könnte das hilfreich sein.

IP-Adressen sind nach Blöcken gemäß CIDR (Classless Inter-Domain Routing) organisiert und hierarchisch gegliedert, sodass man größere Bereiche zusammenfassen und Teil-/Sub-Ranges baumartig einordnen kann – aber nicht muss. IPv4- und IPv6-Blöcke lassen sich parallel und mit gleichem Funktionsumfang verwalten.

## Master, Slaves und Zonen

Um das Hinzufügen weiterer Netzbereiche wie 192.0.2.0/24 zu vereinfachen, kann der Admin beliebig viele eigene Templates anlegen – ideal, wenn man Gateways feste IP-Adressen wie .1 (oder einen Offset zur Netzadresse) zuweisen oder bestimmte Bereiche für das Switch-Management reservieren möchte.

Neben IP- und MAC-Adressen lassen sich mit Proteus eigene DNS-Master- und Slave-Zonen steuern. Auf den Adonis-Servern läuft ein aktueller BIND, sodass der volle RFC-Funktionsumfang des DNS zur Verfügung steht. Die Administrationsoberfläche von Proteus kennt alle RFC-konformen Resource-Record-Typen. Darüber hinaus lassen sich eigene Einträge anlegen.

Wer BIND-Views mag, wird erfreut sein. Proteus bietet sie ebenso wie eine hierarchisch aufgebaute Zonennamen-Verwaltung. So findet man die Zone „example.com“ unter „com“ und darunter „example“. Die Ebenen können beliebig tief verschachtelt sein. Für die kommende Version plant Bluecat die Anzeige als Baumdiagramm.

Ein autoritativer (maßgeblich zuständiger) Nameserver ist besonders für solche Unternehmen wichtig, die ihre Firmen-Domain(s) in Eigenregie verwalten möchten, um unabhängiger vom Hosting-Provider zu sein. Dank der Weboberfläche können sogar BIND-unerfahrene Administratoren damit umgehen. Ein Adonis-Server dient im typischen Setup-Szenario aber meist nicht nur als autoritativer Nameserver, sondern (in der Regel zugleich) als DNS-Resolver/Recursor für die angeschlossenen Clients. Ein sicherheitsbewusster Administrator würde sich hier allerdings wünschen, dass zwei getrennte DNS-Instanzen auf den Adonis-Maschinen zum Einsatz kommen.

Beim an sich unspektakulären DHCP bieten die Adonis-Produkte ein wichtiges Feature, das sich mit Open-Source-Tools nicht ganz einfach lösen lässt: Ein echtes DHCP-Failover, das die bereits vergebenen Leases berücksichtigt.

Für den „Hand-zu-Fuß“-BIND-Administrator sicherlich mit etwas Umstellung verbunden, aber dennoch praktisch und sinnvoll ist die Deployment-Option im Bereich DNS. Alle Änderungen werden nicht sofort auf den angeschlossenen Adonis-Servern aktiv, sondern erst nach einem bewussten „Deploy!“. Das könnte manch inkonsistentes DNS-Setup vermeiden. Auf Wunsch verläuft das Deployment automatisiert und zeitgesteuert, sodass der ohnehin überarbeitete Administrator nicht nachts eine Maustaste betätigen muss.

Die gesamte Webadministration, die wie aus einem Guss erscheint, sowie das dahinterstehende Backend sind laut Hersteller objektorientiert programmiert und umgesetzt. Das merken auch die Anwender. Sämtliche Einträge betrachtet Proteus als eigene Objekte: IP- und MAC-Adressen, Netzblöcke, DNS-Zonen et cetera. So sind auch die bereits beschriebenen Hierarchien auf einfache Weise umzusetzen.

An einem praktischen Beispiel lassen sich die Vor- und Nachteile gut erkennen. So ist der MX-Eintrag in einer DNS-Zone ein eigenes Objekt. Arbeitet in mehreren DNS-Zonen derselbe Mailserver, etwa „mail.example.com“, ändert er sich automatisch in allen Zonen, wenn man ihn zum Beispiel in „mx“ umbenennt. In der Regel ein sinnvolles Feature, allerdings muss der Administrator hier aufpassen, nicht ungewollt mehr Änderungen als nötig vorzunehmen.

## Objektorientierung in Reinstform

Darüber hinaus legt die Objektorientiertheit die Grundlage für eine objektbasierte Rechtevergabe. Man kann in Proteus beliebig viele Benutzer anlegen und deren Rechte in jeder Hinsicht auf ein oder mehrere Objekte beschränken.

So ist ein zweiter Administrator denkbar, der ausschließlich (dort aber uneingeschränkt) auf die IP-Adressen zugreifen darf. Oder einer, der nur DNS-Zonen anlegen und bearbeiten darf. Ebenso ist es möglich und denkbar, Benutzer anzulegen, die nur DNS-Zonen sehen, aber nicht verändern dürfen, etwa Support-Mitarbeiter vom Helpdesk.

Da Proteus eine Art von „View“-ähnlichem Konfigurationskontext realisiert, lassen sich zum Beispiel mehrere Standorte, Firmenteile oder Kunden in einer eigenen „Konfiguration“ verwalten. Zu jeder Konfiguration können mehrere Administratoren, Subadministratoren und so weiter gehören. Hier sind praktisch keine Grenzen gesetzt; die Objekte und deren Hierarchie machen es möglich.

Für jedes Objekt gibt es ein detailliertes Log, das alle Änderungen daran protokolliert – und deren Urheber. Ein automatisiertes Undoing/Rollback-System oder „Snapshotting“ gibt es leider nicht – noch nicht, denn der Hersteller hat solche Funktionen bereits angekündigt.

Zu den überdies erwähnenswerten (von überaus zahlreichen) Funktionen

gehört das Reporting per PDF-Datei, das die Auslastung der IP-Adressblöcke sichtbar macht. Adressbereiche lassen sich aufteilen und zusammenführen. Favoriten ermöglichen jedem Benutzer einen schnellen Zugriff auf persönliche wichtige Einstellungen. Mittels Tagging kann man schnell nach Objekten suchen, ohne durch die GUI navigieren zu müssen.

## Mission: Critical

Redundanz und High Availability spielen gerade in mittleren und großen Unternehmen eine entscheidende Rolle, wenn es um die Auswahl geeigneter Produkte geht. Durch die hierarchische Struktur lassen sich nahezu beliebig viele Adonis-Server einbinden, je nach Konfiguration (im Falle von Master und Slave) sind diese vollkommen redundant und in jedem Falle unabhängig von Proteus.

Auch für Proteus selbst gibt es laut Hersteller ein (Active-Active-)Redundanz-Szenario, etwa in Verbindung mit einem Speichersystem, auf dem die Masterdaten von Proteus liegen (angebunden per iSCSI oder Fibre Channel).

Im Test kamen ein Proteus 5000 sowie zwei Adonis XMB zum Einsatz. Das genutzte Testszenario entspricht laut Hersteller einem Listenpreis von rund 80 000 US-Dollar. Der kleinere Proteus 2150 kostet laut Liste knapp 40 000 US-Dollar, die Adonis-Server rangieren von rund 2000 bis 18 000 US-Dollar. Wie bei derartigen Appliances üblich sind Support, Hardwareservice sowie Updates meist gegen einen jährlichen Support-Vertrag zu erhalten, dessen Kosten vom Kaufpreis abhängen. Erfreulich ist die vom Hersteller angebotene „Evergreen“-Praxis: Er tauscht nicht nur defekte Hardware aus, sondern erneuert die Geräte bei entsprechend langer Vertragslaufzeit alle drei Jahre.

Wer den SSH-Zugang der Maschinen nutzt, stellt fest (wie auch auf der Webseite des Herstellers beschrieben), dass sie auf einem wenig modifizierten Debian-Linux basieren. Lediglich die Kernels der Systeme sind an die speziellen Anforderungen angepasst.

Die Webadministration von Proteus basiert auf einem JBoss-Server. Auf Adonis existiert eine per *iptables* realisierte Firewall, die Systemverwalter um händische Einträge, etwa in Bezug auf Connection-Rate-Limiting, erweitern können.

## Fazit

Adonis und Proteus eignen sich prinzipiell schon für Kleinunternehmen. Sie erleichtern die Arbeit ungemein, sind logisch aufgebaut und daher gut zu verstehen. Durch den Einsatz mehrerer Systeme beider Produktreihen lässt sich eine Redundanz schaffen, die auch für große Unternehmen oder Mission-Critical-Anwendungen geeignet ist.

Lediglich der Preis der Systeme bleibt ein Wermutstropfen. Die meisten kleinen und auch viele mittelständische Unternehmen dürften eine Investition in fünfstelliger Höhe scheuen. Für kleine und mittlere Unternehmen kommt daher eher eine Open-Source-Software mit selbstgeschriebenen Skripts infrage. In größeren Unternehmen könnte sich die Investition aber bezahlt machen und den Systemadministratoren Zeit für spannendere Tätigkeiten verschaffen als das Verteilen und Dokumentieren von IP-Adressen. (un)

### Daten und Preise

**Proteus/Adonis**
Appliances für das IP-Adressmanagement

**Hersteller:** Bluecat Networks, www.bluecatnetworks.com

**Proteus 5000:** Dual-Opteron 270 mit 4 GByte RAM und zwei 73 GByte-SCSI-Festplatten

**Adonis XMB:** Intel Celeron (1 GHz), 512 MByte RAM, eine IDE-Festplatte (40 GByte)

**Listenpreise:** Proteus ab 39 995 US-Dollar, Adonis ab 1995 US-Dollar

**Betriebssystem:** modifiziertes Debian-Linux

### iX-Wertung

⊕ intuitiv benutzbare Oberfläche

⊕ durchdachtes, flexibles Konzept

⊖ hoher Preis

Das Kühlkonzept des neuen Flughafen-RZs Frankfurt



# Saunagang

**Susanne Nolte**

Die Kühlung der IT-Systeme ist nicht nur ein notwendiges Übel, sondern ein energieaufwendiges dazu. Wie man mit einem High-Density-System sparen kann, hat der Frankfurter Flughafen mit der derzeit größten Warmgangeinhausung vorgeführt.

Kaum steigen draußen die Temperaturen, richten sich die besorgten Blicke auf die Klimaanlage der Serverräume. In Rechenzentren dagegen hat das Thema Kühlung ganzjährig Hochsaison. Angeheizt durch steigende Energiekosten und die Klimawandel-Debatte bewegt sich der Fokus weg vom Leistungsvermögen der Klimaanlagen hin zu ihrer Energieeffizienz.

Dabei rücken vor allem physikalische Aspekte in den Vordergrund, die vorher nur wenig Beachtung gefunden haben: Beispielsweise wurde und wird häufig die Serverhalle als Ganzes gekühlt; die Tatsache, dass die großen Luftmengen, die es zu kühlen gilt, den Energieaufwand in die Höhe treiben, wurde dabei ebenso wenig berücksichtigt wie die unterschiedlich temperierten Luftströme, die unterschiedliche Wärmeabgabe der einzelnen Geräteklassen oder die Schwankungen in der Auslastung der IT-Systeme.

Mit dem Einzug von Blade-Servern in Rechenzentren ändert sich das: Die rund um die Blade-Center entstehenden Hotspots zwingen die Verantwortlichen, über neue Kühlkonzepte nachzudenken. Ein Rechenzentrumsbetreiber, der verstärkt auf Blades setzt, ist die Eigentümerin und Betreiberin des Frankfurter Flughafens, die Fraport AG. Im Rahmen eines Neubaus und der Standortverlagerung des in den 70er-Jahren gebauten Rechenzentrums war sie in der Lage, die Infrastruktur den heutigen und künftigen Anforderungen entsprechend neu zu errichten.

Unter anderem ist die Fraport AG zuständig für die Fluginformationssysteme, Bodenverkehrsdienste und Frachtabwicklung, hinzu gesellen sich die interne Bürokommunikation und Verwaltung. Außer ihrem eigenen Personal zählen die Fluggesellschaften, die Flugsicherung, die Bodendienste, Zoll und Bundesgrenzschutz, die Sicherheitsdienste, der Katastrophenschutz, außerdem Mieter und Konzessionäre zu den IT-Anwendern. Ihnen stellt die ITK neben Servern und Anwendungen 4500 PCs, 15 300 Telefone und Faxgeräte, 7900 km Kabel, 99 000 Anschlussdosen, 16 000 LAN-Anschlüsse, 2200 Bündelfunkgeräte samt Infrastruktur, 300 WLAN-Antennen sowie 1260 Überwachungskameras zur Verfügung, begleitet durch 320 Mitarbeiter und durchschnittlich 30 Mio. Euro jährliche Investitionen.

Als für die wachsende Zahl der Anwendungen ein neues Rechenzentrum gebaut werden musste, nahm die Fraport AG im März 2005 auch eine organisatorische Umstrukturierung vor: Als Joint-Venture mit der Gedas (heute T-Systems) gründete sie die Betreibergesellschaft Gedas Operational Services GmbH & Co. KG (Gedas OS) und übertrug ihr das Rechenzentrum.

## Das Haus im Haus

Auf dem Flughafengelände entstand daraufhin bis 2007 ein unterirdisches Rechenzentrum als „Haus im Haus“ mit 1200 Quadratmeter Gesamtfläche. „Das neue Rechenzentrum ist ein sogenanntes Outgrowing-Projekt, das weit über ein gewöhnliches Outsourcing hinausgeht“, so Falk Wieland, Fachgebietsleiter des Rechenzentrums bei Gedas OS. Neben der Absicherung der Fraport-Anwendungen bietet es Managed Services für Fertigungs- und Service-Unternehmen vor allem rund um den Transportsektor an. Unter anderem hat die Gedas die IT-Dienstleistungen für die Volkswagen-Gruppe, deren Zulieferer und Händler mit in die Ehe gebracht.

Aus Sicht der Fraport AG bildet das neue RZ im Wettbewerb der internationalen Luftverkehrsdrehkreuze zum einen ein strategisches Standbein für das Wachstum, zugleich soll es aber auch Einsparungen bewirken. „Die Konsolidierungseffekte der neuen Infrastruktur sollen die IT-Kosten im ersten Jahr um 10 %, langfristig um 30 % senken“, führt Falk Wieland aus. „Um diese Vorgabe erreichen zu können, mussten wir einen Technologiepartner finden, der uns beim Aufbau eines automatisierbaren und hochverfügbaren ‚IT-Hotels‘ unterstützt, das ökonomisch wie ökologisch sinnvoll zu betreiben ist.“

Der Wunschpartner sollte alle Systeme aufeinander abgestimmt und aus einer Hand liefern können, von der unterbrechungsfreien Stromversorgung und -verteilung über standardisierte Rack-

Systeme, Verkabelungslösungen und Kühlkomponenten bis zu Management-Einheiten. Ebenfalls Pflicht war ein zuverlässiges und detailliertes Monitoring. Wieland: „Da unser Rechenzentrum größtenteils autonom arbeitet, bedarf es einer hohen Stabilität ausfallkritischer Kennwerte.“ Die Zusammenarbeit mit dem Rechenzentrumsausstatter sollte sich außerdem über den Zeitraum der Installation hinaus erstrecken. Dabei darf weder der Ausbau der Infrastruktur noch der Austausch von Komponenten die Anwendungen beeinträchtigen.

Entscheidend waren aber auch die Energieeinsparungen. Denn immerhin finden mehr als 50 % der elektrischen Energie nicht den Weg in das IT-Equipment, sondern vielmehr in Kühlung, Stromversorgung und Beleuchtung. 20 bis 30 % ließen sich durch Reihen- oder Rack- statt Raumkühlung, modulare Stromversorgungs- und Kühlanlagen, energieeffiziente USVs und energiesparende Beleuchtung einsparen.

Von großer Bedeutung ist dabei die Skalierbarkeit der Stromversorgungs- und Kühlanlagen: kaum etwas ist unnützer als überdimensionierte Anlagen. Da aber der Bedarf selten an der momentanen IT-Ausstattung, sondern richtigerweise an der zu erwartenden Menge berechnet wird, kann eine skalierbare Anlage, die mit der IT mitwächst, die Energieeffizienz dauerhaft hochhalten. Besteht die Anlage sogar aus mehreren Modulen, kann sie sich zudem der schwankenden Auslastung gerade von High-Density-Servern anpassen, unter Umständen unter Zuhilfenahme einer Kapazitätsplanungs- und -managementsoftware.

## Schlankes Equipment spart Rohstoffe

Die Eingrenzung der Klimatisierung auf die Hauptsünder kann darüber hinaus den Energieverbrauch für die Lüfter drosseln und spart das Be- und Entfeuchten der Luft. Zudem reduziert eine Stromeinsparung in der Infrastruktur die Wärmeentwicklung, was wiederum die erreichbare Serverdichte im Gebäude erhöht.

Ein weiterer Aspekt ist nicht zu vernachlässigen: Ein schlankes und auf den Bedarf angepasstes IT- und Infrastruktur-Equipment spart Rohstoffe. Immerhin verbraucht ein durchschnittliches 1-Megawatt-Rechenzentrum in seiner 10-jährigen Lebenszeit 227 Millionen Liter oder 227 000 $m^3$ Wasser, 65,8 t Kupfer, 9,5 t Blei, 15 t Plastik, 33 t Aluminium, 5,4 t Lötzinn und 171 t Stahl.

Nach öffentlicher Ausschreibung und ausführlicher Evaluierungsphase entschieden sich die verantwortlichen Projektmanager der Gedas os im September 2005 für das modulare Infrastrukturkonzept der Firma APC.

Nach fast einjähriger Bauphase dauerte das anschließende Installieren der ausgewählten Infrastruktur nur zwei Monate. Die wohl größte Herausforderung des Projekts war laut Wieland der Umzug der operativen Flughafen-IT in das neue Rechenzentrum: „Die Arbeiten durften den Betrieb der IT-Systeme des Flughafens zu keinem Zeitpunkt gefährden. Eine weitere Schwierigkeit war, unseren Zeitplan mit dem wechselnden Passagieraufkommen zu koordinieren.“

Heute nehmen ein Viertel der 1200 Quadratmeter im RZ die Systeme für die mittlerweile 120 größeren Anwendungen der Fraport ein, der Rest ist einerseits dem Wachstum des eigenen IT-Bedarfs, andererseits den Drittkunden vorbehalten. In den Racks tummeln sich inzwischen 69 IBM-pSeries-Systeme mit AIX, 20 IBM-SP-Nodes (Scalable Power Parallel) mit AIX, 15 Sun-Solaris-Server, 100 Intel-basierte Blade-Systeme mit Linux und Windows von IBM sowie 90 HP-Proliant-Server mit Windows.

Auf diesen fast 300 Servern, unterteilt in etwa 350 logische Server, laufen etwa 160 Anwendungen, darunter 20 kritische. Die wichtigsten sind die großen SAP-R/3-Installationen auf HP-UX/Oracle, Windows/Oracle und AIX mit Oracle respektive DB2. Die Server beziehen ihren Plattenplatz von zwei IBM-ESS-800-PPRC-Clustern (Peer to Peer Remote Copy) mit 8,4 TByte, zwei separaten IBM ESS 800 mit 13,1 TByte, einer IBM DS 4800 mit 20 TByte und einer HP MSA 1000 mit 6 TByte. Ums Backup kümmern sich zwei 146 TByte fassende IBM 3584 L32 LTO- und eine IBM 7337 DLT-Library.

Die gesamte Hardware verteilt sich auf zwei unterschiedliche Rack-Konstellationen: Zwei offene Rack-Reihen bieten den Systemen mit geringerem Stromverbrauch und niedrigerem Kühlungsbedarf Heimstatt, während die Blade-Server in zwei mehrere Dutzend Meter langen Warmgangeinhausungen, sogenannten High Density HACS (Hot Aisle Containment Systems) wohnen. Zu beiden Seiten des heißen Gangs befinden sich die über dem Gang zu Quadern zusammengeschlossenen und nach außen hin abgeschlossenen Rack-Zeilen. Die zwischen den Serverschränken eingebauten, wassergekühlten Klimaanlagen Inrow FM 40 saugen die warme Luft von dort aus gezielt über den integrierten Wärmetauscher ab. Sie entziehen der Luft die Wärme und befördern sie über einen geschlossenen Wasserkreislauf zum Kaltwassersatz (Chiller) nach außen.

## Warmgang runterfahren

Dieses Kühlkonzept zeitigte schnell Synergieeffekte: „Zwei Monate nach Inbetriebnahme des Rechenzentrums erreichten wir eine planmäßige Auslastung von 20 %“, erklärt Wieland. „Die Klimaeinheiten in den beiden offenen Schrankreihen produzieren allein so viel Kaltluft, dass wir die für die High-Density-Würfel vorgesehene redundante Doppelbodenklimatisierung energiesparend auf Standby-Betrieb beschränken können.“ Bei Bedarf ausbauen lässt sich die Klimaanlage auf eine Kapazität von 1,2 Megawatt, die für die 2+1-Redundanz benötigte Ersatzanlage auf 0,6 Megawatt.

Integriert in die Infrastruxure genannte Gesamtlösung, die aus vernetzten Modulen besteht, sind neben dem Kühlsystem die passenden Racks, die Kabelführungen, die unterbrechungsfreie Stromversorgung und -verteilung von 1,6 Megawatt (3200 Ampere) sowie die Monitoring- und Management-Einheiten. Die wiederum liefern den Operatoren alle nötigen Informationen und gestatten dem Betreiber letztendlich die Automatisierung des Rechenzentrums mit essenziellen Funktionen wie Eskalationslogik, Analysen, Berichten und Vorschlägen zur Beseitigung von Fehlern. Rechenzentrumsleiter Wieland: „Die tiefe Integration der ISX Manager in unsere eigenen Managementsysteme bietet uns einen Echtzeit-Überblick über die gesamte IT-Infrastruktur und liefert damit einen hohen Beitrag zur Gesamtverfügbarkeit von mehr als 99,8 Prozent.“

Als Löschgas steht FM200 bereit. Der international als HFC227ea bekannte teilhalogenisierte Kohlenwasserstoff löscht auf chemischem Weg, das heißt durch Unterbrechung der Verbrennungskette. 45 Kameras überwachen die rollenbasiert gesteuerten Zugänge zu den einzelnen RZ-Bereichen. Zudem sind die Hochsicherheitssegmente biometrisch geschützt. Der Hot-Swap-Ansatz ermöglicht den Austausch essenzieller Module wie Batterien, USV- oder Kühlungseinheiten während des Betriebs. Ergänzend dazu übernimmt APC auf Einjahresbasis die Wartung. (sun)



Was Googles Opensocial-API leistet

# Aufgeschlossen

**Ramon Wartala**

Wer eine Anwendung für StudiVZ, Xing oder ein anderes soziales Netz erstellt hat, möchte sie sicherlich nicht nur einem dieser Netze zur Verfügung stellen. Das erfordert eine API, wie Googles Opensocial sie darstellt.

Googles Opensocial-Programmierschnittstelle ermöglicht es Webentwicklern, ihre Anwendungen für eine Vielzahl sozialer Netze zu erstellen. Über eine gemeinsame Schnittstelle können Programmierer in unterschiedlichen sozialen Netzen einheitlich auf die Daten und Informationen des Nutzers und seiner Freundschaftsbeziehungen zugreifen. Grundlage dafür ist eine von Google entwickelte Container-Architektur, die die teilnehmenden Social Networks implementieren müssen.

Facebook stellt seit dem Frühjahr letzten Jahres seine Entwicklungsschnittstelle Facebook Platform [h] einer breiten (Entwickler-)Öffentlichkeit als Weg vor, eigene Anwendungen in das Facebook-Netz zu integrieren. Die für viele als Revolution gefeierte Öffnung von Facebook erzeugte in kurzer Zeit eine Fülle sinnvoller und freier Anwendungen. Aktuell stehen im offiziellen Facebook-Applikationsverzeichnis 25 000 dieser Anwendungen dem Nutzer zur Verfügung.

Kein halbes Jahr nach diesem medienwirksamen Auftritt verkündete Google an der Spitze eines Konsortiums kleinerer und größerer sozialer Netze die Öffnung dieser Dienste über die gemeinsame Programmierschnittstelle Opensocial. Es handelte sich um Nin, Plaxo, Friendster, Hi5, Orkut, Viadeo, Six apart, Salesforce.com, LinkedIn, Oracle CRM Ondemand, Engage, Bebo, imeem, Hyves, Myspace und Tianji. Deutsche Netze wie Amiando, StudiVZ und Xing schlossen sich der Karawane an. Mittlerweile sind rund 75 Firmen Teil der Opensocial-Partnerliste.

## Container und Applikationen

Die Vorteile für Entwickler liegen klar auf der Hand: Die eigene Applikation muss nur noch eine Schnittstelle implementieren und kann innerhalb einer oder mehrerer sozialer Netze laufen.

**iX-TRACT**

- Innerhalb weniger Tage haben Facebook und Google Schnittstellen für soziale Netze angekündigt.
- Dem von Google initiierten Opensocial haben sich mittlerweile über 70 Firmen angeschlossen, darunter die deutschen Xing und StudiVZ.
- Knappe Listings demonstrieren die Nutzung der Programmierschnittstelle.




**HelloWorld-Gadget innerhalb des iGoogle-Containers (Abb. 1)**

Dabei wartet die Opensocial-API mit genau den gleichen Konzepten auf, die in der Facebook Platform implementiert sind. Ein weiterer Vorteil ist, dass Googles Version über Standard-HTML und Javascript funktioniert und nicht wie Facebook auf proprietäre Techniken wie FBML (Facebook Markup Language), FQL (Facebook Query Language) et cetera setzt. Das hat wiederum den Vorteil, dass Entwickler für derartige Anwendungen gängige Entwicklungswerkzeuge nutzen können. Um das Ganze dennoch sicher zu gestalten, laufen Opensocial-Anwendungen in speziellen Laufzeitumgebungen, Container genannt, ab.

Für Social Networks, die sich der Google-Allianz bereitwillig angeschlossen haben, heißt das im Umkehrschluss, dass sie, um Applikationen ausführen zu können, einen entsprechenden Container zur Verfügung stellen müssen. Sogar dafür hat Google gesorgt und einen Monat nach Ankündigung der Initiative die Referenz-Implementierung eines solchen Containers mit Namen Shindig [i] der Apache Software Foundation (ASF) übergeben (siehe den Kasten „Ein Containerschiff namens Shindig“). Technisch stellt diese Art von Anwendungsarchitektur eine reine Plug-in-API dar, die Marc Andreessen, Mitbegründer von Netscape und Investor von Ning als „Level 2 Platform“ [a] beschreibt. Dabei sind Schnittstellen vom Typ Level 1 reine Zugriffsschnittstellen, über die mit SOAP oder REST auf Daten zugegriffen werden kann. Im Gegensatz dazu kennt man Plug-in-Schnittstellen vor allen Dingen von Desktop-Anwendungen wie Photoshop oder Firefox, wo diese dazu dienen, Funktionen von Drittherstellern zu integrieren.

## Gadgets statt Applikationen

Die Opensocial-API implementiert die schon von der Facebook Platform bekannten Zugriffe [h] auf

– Profil-Informationen der Nutzer,
– Informationen im eigenen Freundeskreis (Social Graph),
– verschiedene Aktionen, die die Nutzer starten können.

**Listing 1: Grundgerüst eines Opensocial-Gadget**

```
1  <?xml version="1.0" encoding="UTF-8" ?>
2  <Module>
3    <ModulePrefs title="Beispiel Opensocial Gadget">
4      // ...
5      <Require feature="opensocial-0.7" />
6    </ModulePrefs>
7    <Content type="html">
8      <![CDATA[
9        <script type="text/javascript">
10         // ...
11       </script>
12       // ...
13     ]]>
14   </Content>
15 </Module>
```

**Listing 2: Ausführung der Methode init() beim Laden**

```
1  // ...
2  gadgets.util.registerOnLoadHandler(init);
3
4  function init() {
5    loadFriends();
6  }
7  // ...
```

**Listing 3: Ermittlung aller Freunde und Datenübergabe**

```
1  function loadFriends() {
2    var req = opensocial.newDataRequest();
4    req.add(req.newFetchPersonRequest('VIEWER'), 'vie-
wer');
5
req.add(req.newFetchPeopleRequest('VIEWER_FRIENDS'),
'viewerFriends');
6    req.send(onLoadFriends);
7  }
```

**Listing 4: Erzeugen einer HTML-Ansicht**

```
1  function onLoadFriends(data) {
2    var viewer = data.get('viewer').getData();
3    var viewerFriends = data.get('viewerFriends').get-
Data();
4
5    html = new Array();
6    html.push('<ul>');
7    viewerFriends.each(function(person) {
8      html.push('<li>' + person.getDisplayName() +
"</li>");
9    });
10   html.push('</ul>');
11   document.getElementById('friends').innerHTML =
html.join('');
12 }
```

## Kampf um Single Sign-On 2.0

Innerhalb weniger Tage im Mai haben sich die Schwergewichte im Kampf um die Vorherrschaft bei den sozialen Netzen einen grandiosen Schlagabtausch geliefert und Produkte angekündigt, die sich von ihren Funktionen her stark ähneln und dasselbe Ziel verfolgen: einen Standard für Single Sign-On in sozialen Netzen zu setzen. Zunächst verkündete Myspace, dem Data-Portability-Projekt [g] beizutreten. Hauptzweck dieses Dienstes soll kurzfristig der einfache Austausch von Myspace-Nutzerprofilen mit Yahoo, Ebay, Twitter und langfristig mit jedem Website-Betreiber sein.

Einen Tag später verkündete Facebook die Einführung des Facebook Connect getauften Dienstes an, der auch den Identitätsaustausch mit anderen Websites ermöglichen soll. Ganze vier Tage später stellte Google mit seinem neuen Dienst Friends Connect ein Produkt vor, das es Website-Betreibern erlaubt, durch über Copy & Paste der eigenen Seite hinzugefügte Code-Schnipsel Funktionen nachzurüsten – Nutzerregistrierung, Einladungen, Fotogalerie für Mitglieder und den Austausch privater Nachrichten. Leider sind nur wenige, konkrete Informationen zu den einzelnen technischen Lösungen zu bekommen. Allein der enge Bezug zur Opensocial-Allianz lässt Google schon jetzt als vermeintlichen Sieger erscheinen. Können doch so die vielen, kleinen Websites ohne zusätzlichen Login-Mechanismus von dem Erfolg der großen sozialen Netzwerke profitieren.




**Soziale Netze und Website-Authentifizierung rücken enger zusammen (Abb. 2).**

**Listing 5: Einbindung externer Datenquellen**

```
1   // ...
2   function makeFeedRequest() {
3           var params = {};
4           params[gadgets.io.RequestParameters.CONTENT_TYPE] = gadgets.io.ContentType.DOM;
5           var url = "http://www.heise.de/newsticker/heise-atom.xml";
6           gadgets.io.makeRequest(url, response, params);
7   };
8   // ...
9   function response(obj) {
10    var domData = obj.data;
11    // ...
12  };
```

Google hat das Architektur-Rad nicht neu erfunden, sondern setzt konsequent auf Vorhandenes. So fungieren als Hülle einer Applikation die von Google bekannten Gadgets [b], die sich in Form von XML-Dateien beschreiben lassen. Gadgets stellen gleichsam kleine, eigenständige Webseiten dar, die eine bestimmte Funktion auf einem klar definierten Raum realisieren. Das Grundgerüst eines Gadget kann man mit einem gewöhnlichen Texteditor erzeugen. Komfortabler geht es mit Googles Gadget Editor (GGE, [c]). Im Inneren eines Gadget werkelt ein Sammelsurium aus HTML und CSS für das Layout und Javascript für die eigentliche Funktion. Gadgets verfügen darüber hinaus noch über die Eigenschaften der Opensocial-Javascript-Bibliothek, die momentan in der Version 0.7 [d] vorliegt. Grob lässt sich die Programmierschnittstelle in zwei Bereiche unterteilen, die jeweils über einen eigenen Javascript-Namensraum voneinander separiert sind:

– *Opensocial*.* enthält alle Funktionen für den Zugriff auf Daten und Aktionen innerhalb des Social Network. Dazu gehören beispielsweise Funktionen für den Zugriff auf Adress-Informationen, Aktionen, Nachrichten et cetera.
– *gadgets*.* enthält Hilfsfunktionen für die Ein- und Ausgabe und die Verwaltung von Gadget-spezifischen Informationen.

## Zur Anatomie der Gadgets

Im Folgenden soll ein kurzes Beispiel einige der Kernfunktionen der Opensocial-API demonstrieren. Ausführen lässt es sich unter den Testumgebungen der jeweiligen Opensocial-Partner [e]. Eine Alternative ist es, lokal die Container-Referenzimplementierung zu installieren. Der Test erfordert allerdings nicht nur die eigentliche Laufzeitumgebung, sondern außerdem einen Ort, von dem aus der Code abgerufen werden kann. In der Regel ist dies ein eigener Webserver. Die Listings dieses Artikels wurden in Googles eigenem Startseiten-Portal, iGoogle, auf der Medienplattform imeem.com und in einer lokalen Shindig-Instanz getestet.

Das Grundgerüst einer Opensocial-Applikation stellt die XML-Datei in Listing 1 dar. Googles Gadget-API [f] beschreibt die Struktur. Innerhalb der Preferences (Zeile 4) können verschiedene, allgemeine Angaben zur eigenen Anwendung stehen. Dazu gehört der obligatorische Titel der Applikation, der Name des Autors oder eine Kurzbeschreibung der Funktionen. Wichtig für ein Opensocial-Gadget ist Zeile 5, die die Version der zu nutzenden API angibt. Zeile 7 und die folgenden enthalten den eigentlichen Inhalt der Anwendung. Der kann aus HTML, CSS-Statements oder eigenem Javascript-Code bestehen, der entweder lokal innerhalb des Content-Bereichs definiert ist oder über einen externen Link eingebunden wird.

## Betrachter, Eigentümer und Freunde

Bei der Entwicklung einer Anwendung ist es wichtig, sich die unterschiedlichen Rollen eines Nutzers vor Augen zu führen. Die Opensocial-API unterscheidet hier zwischen dem sogenannten Betrachter (Viewer) (dem eingeloggten Nutzer auf der Plattform), dem Eigentümer (Owner), dem das Profil gehört, und den Freunden (Friends), die in einer Beziehung zum Eigentümer beziehungsweise Betrachter stehen. Drei Teile sind nötig, Freunde innerhalb einer Anwendung zu ermitteln und darzustellen (Listing 2, 3 und 4).

Der Datenaustausch beschränkt sich nicht auf das zugrunde liegende soziale Netz. Externe Quellen können Entwickler ebenfalls einbinden. Die API ermöglicht es, Daten von externen Systemen aufzurufen – durch die *makeRequest*-Methode aus dem *gadgets.io*-Paket. Die Methode kann sowohl einen *GET*- als auch einen *POST*-HTTP-Request auf eine beliebige URL auslösen. Zurückgeliefert werden die Daten in Form von XML, JSON oder normalem Text-Inhalten. Listing 5 zeigt die Nutzung des Request anhand des *iX*-News-Feeds im Atom-Format.

Innerhalb der Methodenaufrufs *makeRequest* wird als Parameter mit *response* eine Methode übergeben, die sich um

## Ein Containerschiff namens Shindig

Shindig stellt die Referenzimplementierung eines Opensocial-Containers dar, die Google der Apache Software Foundation (ASF) übergeben hat. Sie kommt in zwei Ausprägungen daher. Entweder als Java-Applikation (WAR) oder als PHP-Version. Für die Installation sind eine Java-Runtime-Umgebung ab Version 1.5, ein Subversion-Client und Apaches Maven 2 nötig, für die PHP-Variante Version 5.x der Programmiersprache mit SimpleXML und der JSON-Erweiterung sowie *mod_rewrite* auf der Apache-Seite. Zum Installieren der Quellen reicht ein einfaches Verzeichnis mit Namen *shindig*, um darin den Projekt-Trunk auszuchecken zu können. Der Shindig-Container beinhaltet folgende Komponenten:

– Gadget Server: eine Open-Source-Version von *gmodules.com*, der bei Google das Hosting der zahlreichen Gadgets übernimmt. Der Server übersetzt die XML-Beschreibung der Gadgets in Javascript und HTML für den Gadget-Container.

– Gadget-Container: Kernfunktionen des Javascript-Gadget-Framework. Übernimmt die Aufgaben Layout, Sicherheit, Kommunikation und Erweiterungen wie die der Opensocial API.

– Container für Javascript: enthält spezielle Funktionen der API wie die der Zugriffe auf die Profildaten, den Social Graph und Informationen über Aktionen.

– Data Server: Open-Source-Implementierung der Schnittstelle für containerspezifische Informationen, inklusive der REST-APIs.

Für die lokale Entwicklung von Anwendungen muss nach dem Download das Maven Repository mit *mvn* aufgebaut werden, wobei sämtliche Pakete und Libraries heruntergeladen werden, was je nach Netzanbindung einige Minuten in Anspruch nehmen kann. Unit-Tests überprüfen bei der Installation die Lauffähigkeit der einzelnen Komponenten.

## Onlinequellen

| | |
|---|---|
| [a] Marc Andreessens Blog-Eintrag | blog.pmarca.com/2007/09/the-three-kinds.html |
| [b] Googles Gadget-Spezifikation | code.google.com/apis/gadgets/docs/spec.html |
| [c] Googles Gadget Editor | code.google.com/apis/gadgets/docs/gs.html#Scratchpad |
| [d] Opensocial-API-Spezifikation | code.google.com/apis/opensocial/docs/0.7/spec.html |
| [e] Testumgebungen einiger sozialer Netze | code.google.com/apis/opensocial/getting started.html |
| [f] Googles Gadget XML | code.google.com/apis/gadgets/docs/reference.html#XML_Ref |
| [g] Data-Portability-Projekt | www.dataportability.org |
| [h] Facebook Platform | developers.facebook.com |
| [i] Shindig, Container der Apache Software Foundation | incubator.apache.org/shindig/ |

die Aufbereitung der Daten kümmert. Die Daten selber sind in der Instanz von *obj* verfügbar und über *obj.data* zu bekommen (Zeile 10).

## Fazit

Beeindruckend an Googles Initiative ist nicht nur die Anzahl der Firmen, die sich in der Opensocial-Allianz (gegen Facebook) verschworen haben; hier lässt sich tatsächlich von einem Industriestandard sprechen. Auch die komplette Infrastruktur aus Front- und Backend ist in einer relativ kurzen Zeit entstanden und als Open Source freigegeben. Und dennoch merkt man, dass erst wenige soziale Netze die Opensocial-Spezifikation umgesetzt haben. Lediglich Hi5, Myspace, Hyves, iGoogle, Imeem, Netlog und Orkut können einen standardkonformen Container vorweisen.

Google sollte die Dokumentation der Container-Referenzimplementierung Shindig um weitere Codebeispiele vervollständigen. Hier macht sich an vielen Stellen die rasante Entwicklung der Plattform bemerkbar, die sich wie das Äquivalent von Facebook hier und da durch inkonsistente Dokumentation auszeichnet. Vorteile für Entwickler sind das viel gepriesene „Write once, run anywhere“ und die niedrige Einstiegshürde, die eine rein Javascript-basierte API bedeutet. Bleibt zu hoffen, dass die Mitglieder der Initiative schnell Container für diese spezielle Gadget-Spezifikation zur Verfügung stellen. (hb)


RAMON WARTALA

ist IT-Leiter beim Hamburger Onlinevermarkter orangemedia.de GmbH. Er ist Koautor des Buches „Webanwendungen mit Ruby on Rails“, das 2007 bei Addison-Wesley erschienen ist.

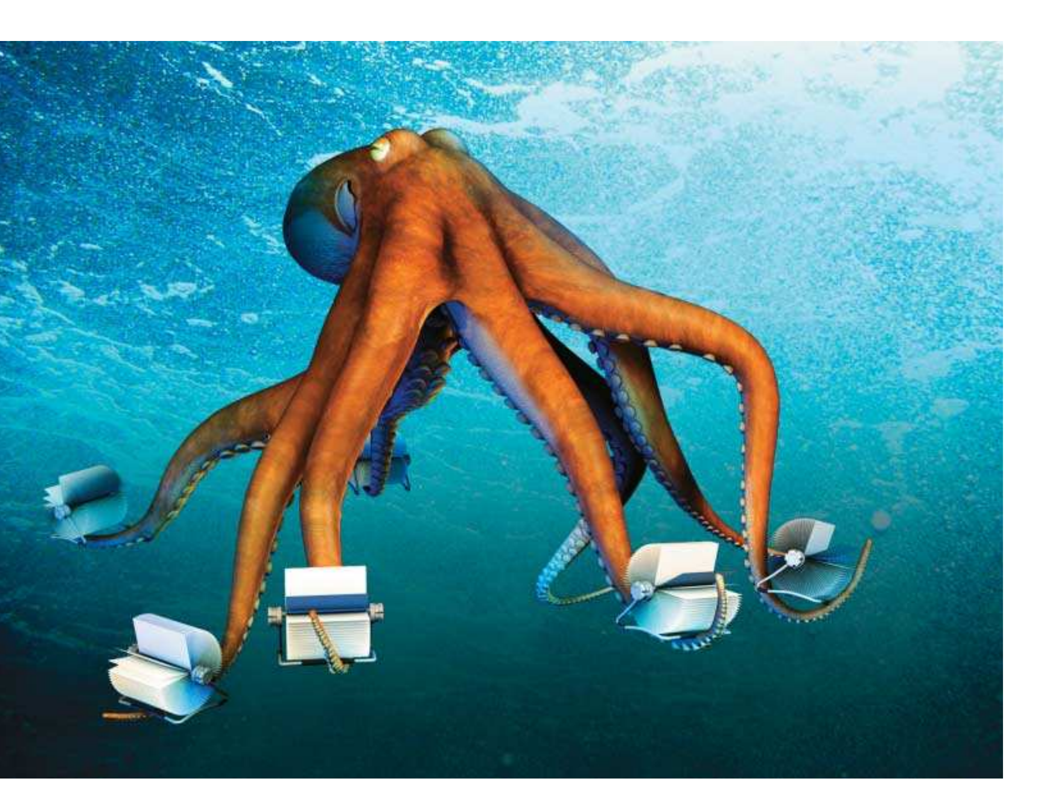

### Literatur


[1] Ramon Wartala; Webschnittstellen; Das eigene Gesicht; Facebook-Applikationen entwickeln; *iX* 4/08, S. 78









Werkzeuge zur datenbankübergreifenden Verwaltung

# Alles mit einem

**Christian Kirsch**

Zwar hätten es die Hersteller relationaler Datenbanksysteme gerne, doch in kaum einem Unternehmen läuft nur das Produkt eines Anbieters. Eine Konsequenz des Artenreichtums sind höhere Verwaltungskosten. RDBMS-übergreifende Werkzeuge können die Arbeit erleichtern und Kosten senken.

Vor gut neun Jahren schrieb Craig S. Mullins: „Die größte Herausforderung, der Datenbankadministratoren gegenüberstehen, ist die Verwaltung heterogener Datenbankumgebungen.“ Er sah für die Zukunft „eine Java-Anwendung im Webbrowser, die objektrelationale Daten von DB2, Oracle und Informix benutzt“ voraus (s. *iX*-Link). „DBAs lösen Änderungen in DB2 und Sybase von einer Management-Konsole aus – ohne Stillstand der Datenbank.“ Ganz sicher war er sich seiner Vision jedoch nicht: Sein Text schließt „Oder träume ich nur …“

Nicht alles war geträumt: Produkte für die Verwaltung unterschiedlicher RDBMS gibt es inzwischen, wenn auch kaum eines in Java geschrieben ist oder im Browser läuft – die Tabelle „Produkte zur herstellerübergreifenden Datenbankverwaltung“ gibt einen Überblick. Und objektrelationale Daten spielen wohl immer noch nicht ganz die Rolle, die Mullins damals erwartet hatte.

Die von ihm beschriebene Herausforderung jedoch bleibt. Denn in vielen Unternehmen laufen Datenbankserver verschiedener Hersteller. Jeder liefert in der Regel seine eigene Verwaltungsoberfläche, die mehr oder weniger komfortables Arbeiten ermöglicht. Administratoren müssen sich folglich für jedes Produkt auf eine neue Umgebung einstellen – aufwendig und fehlerträchtig.

## Kein Ersatz für Detailkenntnisse

Ein einziges Programm, das möglichst viele Details der konkreten Datenbanksysteme abstrahiert, sollte also Zeit und Arbeit sparen. Intensive Einarbeitung in die Details der benutzten RDBMS kann es jedoch nicht ersetzen, denn bei allen Ähnlichkeiten gibt es gerade hinsichtlich der Administration viele Unterschiede, und häufig bezeichnen unterschiedliche Begriffe dasselbe – oder derselbe Begriff benennt etwas anderes.

Eine der einfachsten Aufgaben eines Administrationswerkzeugs ist die Überwachung („Monitoring“) der Datenbankserver. Laufen sie überhaupt, wie viel Speicher- und Plattenplatz belegen sie – Antworten auf diese Fragen sollte es dem Benutzer jederzeit auf Knopfdruck liefern können. Ebenfalls zu den Grundfertigkeiten einer DB-Verwaltung gehört das Starten und Stoppen des Servers per Mausklick.

Logischer nächster Schritt sind automatisch versandte Nachrichten, wenn etwas nicht stimmt: abgestürzte Server, knapp werdender Speicher, voll laufende Tablespaces sind Kandidaten dafür. Einstellen lassen sollte sich, welche Situation eine Meldung auslöst sowie auf welchem Weg sie welchen Empfänger erreicht. Bleibt ein Server hängen oder stürzt gar ganz ab, erwartet man vom Administrationswerkzeug, den Blick in die Log-Datei freigeben zu können. Technisch lässt sich das jedoch nicht für jede Datenbank realisieren. MySQL etwa bietet erst ab Version 5.1.6 die Möglichkeit, Log-Daten in Tabellen zu speichern und so mit beliebigen Datenbank-Clients darauf zuzugreifen. Liegen die Protokolle jedoch in Dateien auf dem Server, auf die das RDBMS keinen Zugriff hat, bleibt auch ein Administrationswerkzeug chancenlos.

## Einschränkungen durch die Datenbank

Vergleichbare Einschränkungen gelten für das dauerhafte Ändern von Server-Parametern im laufenden Betrieb. Bei

Oracle und ähnlichen Produkten ist das ohnehin via Datenbankbefehl möglich, der sich ebenso von einem Werkzeug erzeugen lässt. MySQL benutzt jedoch eine externe Konfigurationsdatei, die meist in */etc/my.cnf* liegt. Sie kann nicht mal ein ohne spezielle Rechte auf demselben Rechner laufendes Programm ändern – von einem remote eingesetzten Tool ganz zu schweigen. Man sollte die Erwartungen an ein herstellerübergreifendes Werkzeug also nicht zu hoch schrauben.

Neben der reinen Überwachung des Servers müssen Administratorinnen regelmäßig wiederkehrende Aufgaben erledigen: Backups erstellen, Indizes reorganisieren, neue Benutzer anlegen. Nur Letzteres lässt sich mit Standard-SQL einigermaßen unabhängig von der Datenbank erledigen, denn die dafür nötigen *GRANT*- und *REVOKE*-Befehle dürfte jedes Produkt heutzutage kennen. Auf sie können Verwaltungswerkzeuge für die einfache Aufgabe zurückgreifen, einem Benutzer Rechte zuzubilligen oder zu entziehen. Darüber hinausgehende Konzepte wie Rollen und Benutzergruppen gibt es jedoch nicht überall. Sie in der Verwaltungsoberfläche umzusetzen gehört deshalb schon zur wünschenswerten Kür.

Noch größer als bei der Benutzerverwaltung dürften die Unterschiede zwischen den Datenbanken ausfallen, wenn es ans Innenleben geht. So lässt sich bei dem einen RDBMS bis hinunter zur Blockgröße alles Mögliche einstellen, ein anderes versucht, die besten Parameter automatisch zu bestimmen. Manche Server führen Abfragen besonders schnell aus, wenn man ihnen aktuelle Statistiken, das heißt Informationen über die Datenverteilung, zur Verfügung stellt.

## Nicht nur für Verwaltungszwecke

Unabhängig von diesen Unterschieden im Detail gehören Datensicherung und -wiederherstellung zu den unabdingbaren Aufgaben des DBA. Für beides sollte das Werkzeug geeignete Funktionen bieten, die regelmäßige oder manuelle Backups ebenso ermöglichen wie das (selektive) Zurückspielen der Sicherung.

Jenseits der Administration im engeren Sinne lassen sich viele datenbankunabhängige Werkzeuge für Wartungs- und Entwicklungsarbeiten nutzen. Eine relativ einfache Aufgabe ist der Vergleich von Datenbankobjekten, etwa zur Untersuchung verschiedener Versionsstände eines Systems. Der nächste Schritt ist das Migrieren einer ganzen Datenbank oder einiger ihrer Teile auf einen anderen Server – sei es zu Testzwecken, um die Entwicklungsumgebung in den Produktivbetrieb zu überführen oder um von einer Version des RDBMS auf die nächste zu aktualisieren. Handelt es sich um Produkte desselben Herstellers, lässt sich die Aufgabe möglicherweise sogar mit dessen Bordmitteln erledigen. Wer jedoch von DB2 zu Oracle oder von MySQL zu PostgreSQL wechseln möchte, dürfte sich über Automatisierung durch ein Werkzeug freuen. Im besten Fall erledigt es alle nötigen Schritte von der Erzeugung der Tabellen, Indizes, Stored Procedures und so weiter bis zum Befüllen mit Daten selbsttätig. Weniger komfortabel, aber immer noch hilfreich sind Ex- und Import-Scripts mit den benötigten SQL-Kommandos. Am Ende der Skala finden sich Produkte, die lediglich das Sichern und Wiedereinspielen der Daten als CSV- oder Text-Datei ermöglichen.

Zwischen Administration und Entwicklung bewegt sich die Arbeit mit SQL-Queries und Stored Procedures. Zwar bringen alle Datenbankserver eine Konsole mit, in der sich Abfragen ausprobieren lassen, deren Komfort ist jedoch recht gering. Eine Rückschau der Queries, nachträgliches Editieren und Speichern sowie Laden erleichtern die Arbeit mit der Abfragesprache erheblich. Solchen Komfort bieten die meisten Verwaltungs-Tools.

Mit Stored Procedures lassen sich etwa das Anlegen neuer Tabellen und die Vergabe von Rechten an ihnen ebenso automatisieren wie komplexe Abfragen zentralisieren. Die meisten Produkte bieten deshalb Editoren für die Prozedursprache(n) an, die über die heutzutage üblichen Fähigkeiten wie Syntax-Hervorhebung und Code-Vervollständigung verfügen. Deutlich schlechter sieht es hingegen mit der Anbindung an Quellcode-Verwaltungen aus. Gerade mal ein Produkt bietet dieses Merkmal, das bei herkömmlichen Entwicklungsumgebungen schon länger zum Standard gehört.

Etwas besser steht es mit der Fehlersuche in Stored Procedures – etliche Produkte bringen einen Debugger mit. Allerdings gibt es diese Programmierhilfe häufig nicht für jede unterstützte Datenbank. Das dürfte daran liegen, dass nicht jedes RDBMS die nötigen Mechanismen wie Haltepunkte, schrittweise Ausführung und Variablenüberwachung bereitstellt, an die externe Werkzeuge andocken können.

In erster Linie für Entwicklerinnen wichtig ist die Möglichkeit, Ausführungspläne von SQL-Statements ansehen zu können. Diese Auswertungen zeigen, mit welchen Teilen einer Abfrage der Server besonders viel Zeit verbringt und wo folglich Verbesserungen sinnvoll sind. Je komplexer die Abfragen, desto undurchsichtiger jedoch der Ausführungsplan. Deshalb ist seine Ausgabe nur die halbe Miete, hilfreicher ist ein integriertes Werkzeug zur Analyse. Es sollte Hinweise darauf geben, wie sich durch Änderungen der SQL-Befehle oder der Datenstruktur das Tempo steigern lässt.

An Geschwindigkeit im Allgemeinen haben auch Administratoren Interesse. Sie sind dafür verantwortlich, dass alle Anwendungen hinreichend zügig laufen. Um das beurteilen zu können, benötigen sie unter anderem Informationen über den Zustand und Durchsatz des Datenbankservers: Wie viele Verbindungen sind gleichzeitig aktiv, wie viele Ein-/Ausgabeoperationen finden statt, wie viele Queries verarbeitet das RDBMS pro Zeiteinheit. All diese Kennzahlen sollte die Verwaltungszentrale liefern können.

So hilfreich ein GUI in vielen Situationen ist, gibt es doch immer wieder Aufgaben, bei denen es im Wege steht. Dazu gehören etwa das Anlegen vieler neuer Benutzer samt Definition ihrer

### iX-TRACT

- Datenbankunabhängige Verwaltungswerkzeuge erlauben das Administrieren verschiedener RDBMS-Systeme mit einer einheitlichen Oberfläche.
- Die Produkte müssen einerseits möglichst viele Einstellungen jedes Datenbankservers zugänglich machen und andererseits die Unterschiede zwischen ihnen ausgleichen.
- Einige Werkzeuge erlauben neben der Verwaltung der Server auch Datenbankentwicklung, da sie einen Editor für Stored Procedures und andere Tools mitbringen.

## Produkte zur herstellerübergreifenden Datenbankverwaltung

| Produkt und Version | Aqua Data Studio 6.5.9 | DBControl 3.0 | Surveillance 4.0 | dbAnalyst 3.7.0.11 |
|---|---|---|---|---|
| Firma | AquaFold | Bradmark Technologies | Bradmark Technologies | Seabird Software LLC |
| unterstützte Betriebssysteme | Windows, Mac OS X, Linux, Solaris, Java | Windows (2000, 2003, XP, Vista), HPUX, AIX, Linux, Solaris, True64 | Windows (2000, 2003, XP, Vista), HPUX, AIX, Linux, Solaris, True64 | Windows (2000, 2003, 2008, XP, Vista) |
| unterstützte RDBMS | Oracle, DB2, SQL Server, Sybase ASE, Sybase IQ, Sybase ASE, Informix, MySQL, PostgreSQL | Oracle bis 11, DB2 UDB 7 bis 8 | Oracle 8 bis 11, DB2 UDB 7 bis 8, SQL Server 7 bis 2005, Sybase ASE 12 bis 15, Sybase Rep Sybase IQ | Oracle 8 bis 10, SQL Server 7 bis 2005, PostgreSQL 7.1 bis 7.4, MySQL 4, DB2 8, Sybase iAnywhere 8, Caché 5, dBase, Text-Dateien, SAP MaxDB 2.6, Ingres 2006 |
| Schemata anzeigen | ✓ | ✓ | – | ✓ |
| Objektabhängigkeiten anzeigen | ✓ | ✓ | – | ✓ [4] |
| Objekte erzeugen | Tabellen, Views, Indizes, Trigger, Stored Procedures [1] | Tabellen, Views, Stored Procedures, Indizes | – | ✓ |
| Objekte verändern/löschen | Tabellen, Views, Indizes, Trigger, Stored Procedures | ✓ | – | ✓ |
| Schemata in einem RDBMS vergleichen | ✓ | ✓ | – | ✓ |
| Schemata in unterschiedlichen RDBMS vergleichen | ✓ | – | – | ✓ |
| Strukturen zwischen RDBMS ex-/importieren | – | – | – | ✓ |
| Daten zwischen RDBMS ex-/importieren | ✓ | – | – | ✓ |
| Editor für Stored Procedures | PL/SQL (Oracle), TSQL (MS SQL Server & Sybase), Standardsprachen für DB2 und PostgreSQL | PL/SQL | – | ✓ |
| Debugger für Stored Procedures | ✓ [2] | – | – | – |
| Datenexport (Formate) | Text, CSV, XML, Excel, Text von INSERT-Statements | – | – | ✓ |
| Datenimport (Formate) | Text, CSV | – | – | – |
| SQL-Konsole/-Editor | ✓ | – | – | ✓ |
| Hervorhebung/Kommandovervollständigung | ✓ | – | – | ✓ |
| Integration mit Quellcodeverwaltung | ✓ | – | – | – |
| Query-Plan zeigen/analysieren | ✓ [3] | zeigen | – | ✓ |
| Serverstatus zeigen/ändern | ✓ | zeigen | zeigen | – |
| Performance-Maße | ✓ | – | ✓ | – |
| Alarmmeldungen an DBA schicken | – | ✓ | ✓ | – |
| Backup/Restore | – | – | – | – |
| Benutzer-/Rollen-Management | ✓ | ✓ | – | ✓ |
| per Skript steuerbar | ✓ | ✓ | ✓ | ✓ |
| Sprache(n) der Oberfläche | en | en | en | en |
| Preis (zzgl. MwSt.) | 399 US-$/Single User License | k. A. | k. A. | 20 US-$ |
| Website | www.aquafold.com | www.bradmark.de | www.bradmark.de | www.seabirdsoftware.com |

[1] für einzelne RDBMS weitere Objekte, unter anderem Datentypen, [2] für Oracle und Sybase ASE, [3] für Oracle, DB2 und SQL Server, [4] mit Abhängigkeitsgraph, [5] nur 32-Bit-Architekturen, [6] mit Zusatzprodukt möglich, [7] Zeigen/Ändern für SQL Server, Zeigen für Oracle, [8] alle Versionen, [9] abhängig vom RDBMS, [10] Oracle, Firebird und Interbase

Rechte und das Sichern von Daten. Ständig wiederkehrende Klicks nerven und kosten Zeit. Für solche Anwendungen ist es deshalb sinnvoll, wenn sich die Verwaltungssoftware per Skriptsprache steuern lässt. Dies erlaubt die Mehrzahl der Produkte.

So groß auch teilweise die Zahl der unterstützten Datenbanken ist, bei den Plattformen herrscht wenig Auswahl. Bis auf ein in Java geschriebenes laufen alle Produkte ausschließlich auf Windows. In der Praxis dürfte dies angesichts der Verhältnisse auf dem Desktop allerdings kaum eine Einschränkung darstellen.

## Fazit

Datenbankübergreifende Verwaltungswerkzeuge müssen dem Administrator einerseits möglichst viele Einstellungen der unterstützten RDBMS zur Verfügung stellen und andererseits die Unterschiede zwischen den Servern nivellieren. Trotzdem kommt der Administrator ohne vertiefte Kenntnisse der einzelnen Produkte nicht aus. Dieses Dilemma mag eine Ursache dafür sein, dass unter anderem Quest und Navicat keine übergreifenden Administrationstools anbieten, sondern für jede Datenbank spezialisierte Lösungen. (ck)

iX-Link ix0807094

| | | | | |
|---|---|---|---|---|
| **DBArtisan 8.5.2** | **EMS SQL Management Studio 1.1** | **EMS SQL Manager 4.3** | **AnySQL Maestro 8.2** | **Database Workbench v3.1** |
| Embarcadero Technologies | EMS Database Management Solutions, Ltd. | EMS Database Management Solutions, Ltd. | SQL Maestro Group | Upscene Productions |
| Windows (2000, 2003, XP, Vista) [5] | Windows | Windows | Windows (2000, XP, Vista) | Windows ab 2000 |
| DB2 LUW, OS/390 und z/OS 8.x/ 9.x, SQL Server 2000/2005 (alle Ausgaben), MySQL 4.x, Oracle 8i bis 11g, Sybase ASE 12.5 bis 15.x | MySQL, SQL Server, PostgreSQL, Interbase/Firebird, Oracle [8] | MySQL, SQL Server, PostgreSQL, Interbase/Firebird, Oracle, DB2 [8] | alle per ADO-Schnittstelle zugänglichen Datenbanken | Oracle (8.1 bis 11), SQL Server (7 bis 2005), MySQL (4.0 bis 5.1), Firebird (1 bis 2.1), Interbase (5 bis 8), NexusDB (2); beliebige ODBC- oder ADO- Verbindungen für Abfragen und Metadaten-Anzeige |
| ✓ | ✓ | ✓ | ✓ | ✓ |
| ✓ | ✓ | ✓ | ✓ | ✓ |
| ✓ | ✓ | ✓ | Tabellen, Indizes, Views | Tabellen, Views, Materialized Views, Indizes, Constraints, Trigger, Objekttypen, Domains, Stored Procedures, Stored Functions, Packages, Java-Quellcode, Assembly/External Library Registrations, Exceptions, Jobs/Events et cetera |
| ✓ | ✓ | ✓ | Tabellen, Indizes, Views | wie oben |
| – [6] | ✓ | ✓ | – | ✓ |
| – [6] | – | – | – | ✓ |
| ✓ | ✓ | ✓ | – | ✓ |
| ✓ | ✓ | ✓ | Export | ✓ |
| PL SQL, T-SQL, IBM SQL | ✓ | ✓ | – | ✓ |
| ✓ | ✓ | ✓ | – | ✓ [10] |
| Text, CSV, XML | Access, XLS, RTF, HTML, XML, PDF, TXT, CSV, DBF, ODF | Access, XLS, RTF, HTML, XML, PDF, TXT, CSV, DBF, ODF | XLS, RTF, HTML, XML, Text, SQL, CSV, LaTeX | CSV, INSERT-Script, XML, XLS, DBF, Text, DIF, Lotus 1-2-3 |
| SQL, TAB, CSV, XLS | Access, XLS, RTF, HTML, XML, PDF, TXT, CSV, DBF, ODF | Access, XLS, RTF, HTML, XML, PDF, TXT, CSV, DBF, ODF | XLS, CSV, Text | CSV |
| ✓ | ✓ | ✓ | ✓ | ✓ |
| ✓ | ✓ | ✓ | ✓ | ✓ |
| – | – | – | – | – |
| zeigen | ✓ | ✓ | – | zeigen |
| ✓ [7] | ✓ | ✓ | – | zeigen |
| ✓ | – | – | – | ✓ [9] |
| ✓ | ✓ | ✓ | – | – |
| ✓ für SQL Server | ✓ | ✓ | – | – |
| ✓ | ✓ | ✓ | – | ✓ |
| – | ✓ | ✓ | – | – |
| en | en, de, fr, ru | en, de, fr, ru | en, fr, de | en |
| 271–10869 Euro | ab 395 € inkl. 1 Jahr Wartung | ab 145 € inkl. 1 Jahr Wartung | Freeware | 118–529 € |
| www.embarcadero.com | www.sqlmanager.net/de | www.sqlmanager.net/de | www.sqlmaestro.com/products/anysql/maestro/ | www.upscene.com/products/dbw/index.htm |



Datenschutzrecht in der Softwareentwicklung

# Vorgebaut

**Tobias Haar**



Wer bei der Softwareentwicklung datenschutzrechtliche Vorgaben berücksichtigt, unterstützt seine Kunden beim Schutz personenbezogener Daten und verschafft sich selbst Vorteile bei der Vermarktung der eigenen Produkte.

Microsoft hat die Bedeutung des Datenschutzes bei der Softwareentwicklung erkannt und 2006 erstmals die „Privacy Guidelines for Developing Software Products and Services" veröffentlicht. Ausgerechnet Microsoft möchte man sagen. Selbstverständlich steckt dahinter wirtschaftliches Kalkül, aber das alleine macht die Herausgabe von Datenschutzrichtlinien für die Softwareentwicklung ja nicht zu einem unglaubwürdigen Unterfangen. Im Gegenteil, man muss den Redmondern bescheinigen, hier die Zeichen der Zeit erkannt zu haben.

Der Datenschutz fristet gerade nach Meinung vieler Datenschützer zwar immer noch ein kümmerliches Dasein, dennoch tut sich in dieser Hinsicht einiges. Die Gesetzgeber führen Audits ein, mit denen man seine unternehmerischen Prozesse, aber eben auch eigene Softwareprodukte auf Einhaltung datenschutzrechtlicher Vorgaben hin untersuchen und zertifizieren lassen kann.

Dass solche Zertifikate bei der Vermarktung der eigenen Produkte helfen können, beweist nicht zuletzt wieder ein Beispiel von Microsoft. So hat das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) den „Windows Update Service" der Redmonder ausgezeichnet und diesem Anfang 2007 das „ULD-Datenschutz-Gütesiegel" verliehen.

In seiner Laudatio äußerte Thilo Weichert, Leiter des ULD, die Hoffnung, dass diese Verleihung eines Gütesiegels Anlass sein könnte, sich von Vorurteilen zu verabschieden. „Leider ist heute immer noch die Ansicht weit verbreitet, dass es sich beim Datenschutz um ein vielleicht notwendiges, aber technikbehinderndes Übel handelt, das irgendetwas mit Grundrechtsschutz zu tun hat. Nicht weniger verbreitet ist die Anschauung, dass Verbraucher- und Grundrechtsschutz umso weniger eine Rolle spielten, je größer und mächtiger eine Institution oder ein Unternehmen ist, schon gar, wenn diese Stelle ihren Sitz in den USA hat", so Weichert.

## Selbstbestimmung im Vordergrund

Microsoft hat mit den Datenschutzrichtlinien nicht zuletzt auf eine zunehmend kritischere Kundschaft Rücksicht genommen. Viele stellen gerade in den USA eine wachsende Bedeutung datenschutzrechtlicher Themen fest und vermuten dahinter nicht zuletzt die drastisch gestiegene Überwachung durch staatliche Institutionen. In diese Kerbe hat Microsoft zunächst mit Forderungen nach einem einheitlichen US-amerikanischen Datenschutzrecht geschlagen und sodann die Entwicklungsrichtlinien folgen lassen.

Das erklärte Ziel der Richtlinien ist es, den Kunden beziehungsweise Nutzer in die Lage zu versetzen, selbst über die Speicherung, Nutzung und Übermittlung personenbezogener Daten zu bestimmen. Das gelingt aber nur, wenn der Softwarehersteller ihm dafür entsprechende Instrumente an die Hand gibt.

Microsoft hat sich mit den Richtlinien quasi ein eigenes Datenschutzgesetz geschaffen. Inhalt und Aufbau der Richtlinie sind insoweit eindeutig. Einem Weltkonzern wie Microsoft kann es nur dann gelingen, weltweit ein datenschutzrechtlich anerkanntes Niveau einzuhalten, wenn dieses idealerweise überall gleich hoch (oder tief) ist. Indem der Softwarehersteller auf seinem größten Markt – den USA – die voraussichtlich ohnehin nicht vermeidbare Diskussion um die Schaffung datenschutzrechtlicher Spielregeln in die Hand nimmt und sich dabei ganz offensichtlich an den gesetzlichen Regelungen in anderen Staaten oder der EU orientiert, machen sich die Redmonder gleichzeitig weniger angreifbar gegenüber der Kritik von außen.

## Mehr Schutz erwünscht

Ganz selbstverständlich verwendet die Richtlinie daher Datenschützern bestens bekannte Begriffe wie personenbezogene oder sensible personenbezogene Daten. Aber die Richtlinie geht noch weiter und berücksichtigt andere Informationen, die an sich nicht dem europäischen Datenschutzverständnis entsprechen, bei denen man sich aber durchaus einen solchen Schutz wünscht. So werden auch Informationen erfasst, die einen Identitätsdiebstahl erst ermöglichen oder vereinfachen, oder solche, die einen Zugang zu geschützten Bereichen gestatten. Der oft zur Identifizierung verwendete „Mädchenname der Mutter" zählt danach genauso zum geschützten Bereich wie Passwörter, PIN-Nummern und dergleichen.

Bedeutsam ist, dass sich die Richtlinien den Grundsätzen der Datenvermeidung und der Datensparsamkeit verschreiben. So soll die eingesetzte Software Nutzer darauf hinweisen, wenn ihre personenbezogenen Daten durch Metadaten mit Dokumenten verknüpft werden und Dritte hierdurch von

ihnen Kenntnis erlangen können, ohne dass dies dem Nutzer bewusst ist. Kernsatz der Richtlinie ist aber, dass der Softwareentwickler bereits in einem frühen Stadium darauf achten soll, ob und in welchem Umfang personenbezogene Daten für die Nutzung der Software überhaupt erforderlich sind und für welche Zwecke sie benötigt werden.

Die Richtlinie sieht vier Schritte zur Erreichung dieser Ziele vor: Es sollen nur personenbezogene Daten verwendet werden, die zwingend erforderlich sind; auf sensible Daten soll man verzichten (Schritt 1). Zugriffsrechte werden nach dem „Need-to-know"-Prinzip vergeben (Schritt 2). Durch Pseudonymisierung und andere Instrumente will man die Informationsdichte verringern (Schritt 3). Und schließlich sollen Speicher- und Löschfristen sowie Löschkonzepte eingeführt werden (Schritt 4).

Kritisieren kann man allerdings die von Microsoft eingeführte dreigliedrige Einwilligungsmöglichkeit: Das Unternehmen unterscheidet zwischen Opt-in, implizitem Opt-in und Opt-out zur Verwendung personenbezogener Daten. Implizites Opt-in und Opt-out – die so im deutschen Datenschutzrecht gar nicht vorkommen – bergen aber die Gefahr, dass der Softwarehersteller den Datenschutz einfach nur dadurch umsetzt, dass er zunächst davon ausgeht, der Nutzer stimme einer Verarbeitung personenbezogener Daten implizit zu. Oder er räumt ihm das Widerspruchs-(Opt-out-)Recht an einer nur schwer zu findenden Stelle ein.

Der allgemeine Teil der Richtlinie befasst sich im Schwerpunkt noch mit IT-Sicherheit und den datenschutzrechtlichen Aspekten beim Shared Computing sowie bei Webseiten und Webdiensten. Hier wirbt Microsoft offen für den P3P-Standard, der Plattform des Privacy Preferences Project, mit der Webseiten die Erhebung und die Nutzung personenbezogener Daten in XML-Format kodieren können. Insbesondere wird die Veröffentlichung einer „P3P Policy" empfohlen.

## Zahlreiche datenschutzrelevante Szenarien

Der dritte und letzte Teil der Policy beschreibt anhand von insgesamt neun Anwendungsszenarien, wie die datenschutzrechtlichen Vorgaben bei der Softwareentwicklung konkret umgesetzt werden sollen. Microsoft bleibt hier bewusst abstrakt und nimmt wenig Bezug auf eigene Produkte, um die Richtlinien auch für andere nutzbar zu machen. Es finden sich folgende datenschutzrelevante Anwendungsszenarien: Übermittlung personenbezogener Daten auf das und vom IT-System des Nutzers, die Speicherung solcher Daten auf dem IT-System des Nutzers, Übermittlung anonymer Daten vom IT-System des Nutzers, die Installation von Software auf einem System, Entwicklung von Webseiten, Speicherung und Verarbeitung personenbezogener Daten in einem Unternehmen, ihre Übermittlung aus einem Unternehmen, der Umgang mit solchen Daten auf Webseiten, die sich an Kinder richten, sowie der Umgang mit personenbezogenen Daten und ihrer Speicherung auf Servern in Unternehmen.

Wie erwähnt, nützt der höchste Aufwand zur Einhaltung datenschutzrechtlicher Standards wenig, wenn sich die erforderlichen Investitionen nicht auszahlen. Gütesiegel, wie sie hierzulande etwa das Land Schleswig-Holstein ausgibt, sind sicher hilfreich. Auch im Bundesdatenschutzgesetz sind freiwillige Datenschutzaudits erwähnt. In § 9a heißt es dazu: „Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen."

Derzeit arbeitet der Gesetzgeber an einem Bundesgesetz, das die Einzelheiten hierzu regeln wird. Gutachter sollen nach dem Gesetzesentwurf der Bundesregierung Zertifikate für die Vereinbarkeit mit datenschutzrechtlichen Vorgaben ausstellen können, die zwei Jahre lang Gültigkeit haben. Beim Bundesdatenschutzbeauftragten soll es ein zentrales Datenschutz-Auditregister geben, in dem sämtliche Zertifizierungen zu hinterlegen sind. Der Missbrauch von Datenschutzsiegeln soll mit Bußgeldern bis zu 250 000 Euro oder bei Betrugsabsicht sogar mit einer Freiheitsstrafe von bis zu zwei Jahren oder einer Geldstrafe bestraft werden.

Wann das Gesetzgebungsverfahren abgeschlossen sein wird, ist noch ungewiss. Leider hat sich der Gesetzgeber hier wieder einmal sehr viel Zeit gelassen. Die Vorschrift zum Datenschutzaudit im Bundesdatenschutzgesetz stammt immerhin schon aus dem Jahr 2001. Ähnliche Vorschriften existieren übrigens nach dem Rundfunkstaatsvertrag, dem Sozialgesetzbuch sowie dem Mediendienstestaatsvertrag. Wirtschaftliche Bedeutung kommt solchen Audits insbesondere dann zu, wenn die öffentliche Hand bei staatlich geförderten IT-Projekten ein Audit- oder Gütesiegelverfahren verlangt.

## Fazit

Nicht nur theoretisch stellen die Entwickler-Richtlinien zum Datenschutz von Microsoft eine beachtliche Selbstverpflichtung dar. Werden sie optimal umgesetzt, ist im Bereich des Datenschutzes bei Microsoft-Programmen viel erreicht. Es wäre wünschenswert, dass andere Softwarehersteller den Redmondern nacheifern.

Allein mit der Veröffentlichung einer solchen Richtlinie ist es aber nicht getan. Man darf nicht vergessen, dass es sich hier um „private Richtlinien" handelt, die staatlich nicht durchgesetzt werden können. Ob ausreichende Taten folgen werden, bleibt abzuwarten. Gerade die jüngsten Vorhaben von Microsoft, die sich verstärkt auf das Internet und dort auf datenintensive Geschäftsmodelle stützen, machen etwas stutzig. Immerhin aber hat Microsoft für den Windows Update Server eines der ersten Datenschutz-Gütesiegel für ein Softwareprodukt in Deutschland erhalten.

Für Unternehmen – gleich ob sie Software entwickeln und anschließend vertreiben oder solche sind, die Software „nur" einsetzen – hat das Land Schleswig-Holstein bereits die Möglichkeit zur datenschutzrechtlichen Zertifizierung geschaffen. Bald ist auch für den Anwendungsbereich des Bundesdatenschutzgesetzes mit der Regelung der Details zum Datenschutzaudit zu rechnen. Zertifizierte Unternehmen sollen mit dem Zertifikat werben dürfen, was den Anreiz zur Auditierung stärken soll.

Bei öffentlichen IT-Vergaben ist in Zukunft verstärkt damit zu rechnen, dass eine solche Zertifizierung ein wesentliches Kriterium bei der Vergabeentscheidung spielen wird. Nicht zuletzt hilft ein Softwarehersteller, der seine Produkte zertifiziert hat, auch seinen Unternehmenskunden, wenn sich diese wiederum zertifizieren lassen wollen. Ebenfalls ein erwünschter Anreiz. (ur)

TOBIAS HAAR, LL.M.,

ist Rechtsanwalt mit Schwerpunkt IT-Recht.





Unerlaubte WLAN-Zugänge ausfindig machen

# Eingefangen

**Marcel Knop, Michael G. Kaiser**

Die technischen Sicherheitsschwächen von Wireless LANs gelten als beseitigt. Was bleibt, sind Anwenderfehler wie das unautorisierte Installieren unzureichend gesicherter WLAN-Hardware im Unternehmensnetz. Wardriving als Gegenmaßnahme hat sich in der Praxis als aufwendig, unzuverlässig und teilweise rechtlich heikel erwiesen. Doch fremde WLAN-Komponenten lassen sich auch übers LAN lokalisieren.

Der physische Zugang zu Funknetzwerken lässt sich nur mit sehr aufwendiger Abschirmung oder durch Störsender verhindern. Dies ist im größeren Maßstab, etwa auf einem großflächigen Firmengelände, nicht zu leisten und schränkt in der Regel auch die Anwender autorisierter Funktechniken ein. Als Lösungen für dieses Problem entstanden seit der Einführung des WLAN-Standards IEEE 802.11b im Jahr 1999 eine Vielzahl von Mechanismen, die einen unautorisierten Zugriff auf logischer Ebene verhindern sollen.

Positiv- oder Negativlisten können bestimmte MAC-Adressen für eine Verbindung mit dem Access Point (AP) vorsehen oder sie davon abhalten. Da allerdings die Adressen zugelassener Geräte unverschlüsselt sind, handelt es sich nur um einen Schutz vor zufälligem Eindringen. Ein gezielter Einsatz von WLAN-Sniffern kann Geräte mit Zugangsberechtigung inklusive ihrer MAC-Adresse ermitteln. Der Angreifer könnte die Adresse seines WLAN-Interface auf eine berechtigte ändern und so die Zugriffskontrolle umgehen.

## Verschlüsselung nicht auf Draht

Wired Equivalent Privacy (WEP) war das erste Protokoll zum Schutz von WLANs, das weite Verbreitung fand. Wegen US-amerikanischer Exportverbote für Verschlüsselungsprodukte mit Schlüssellängen von mehr als 40 Bit und mehrerer Designfehler galt es allerdings schon 2001 als geknackt. Moderne Desktop-PCs können WEP-Schlüssel in wenigen Minuten errechnen. Daher ist WEP heute unabhängig von der Schlüssellänge unsicher.

Erst Wireless Protected Access (WPA/WPA2) brachte ein Protokoll, das drahtlose Netze auf ein vergleichbares Sicherheitsniveau hebt wie kabelgebundene Netze. Damit ist eine Absicherung von Firmen-WLANs gegen Angriffe von außerhalb heute technisch relativ einfach durchführbar.

Die Praxis hat allerdings ein weiteres Risiko aufgezeigt, das die technischen Sicherungen nicht abdecken und das sich oft der Kontrolle der IT-Verantwortlichen entzieht: Das Installieren unautorisierter WLANs durch eigene Mitarbeiter, Besucher oder externe Dienstleister.

## Unautorisierte WLAN-Zugänge

Access Points für WLANs sind heute Massenware mit niedrigen Anschaffungskosten. APs für Privatkunden sind auf einfaches Handhaben und Konfigurieren hin optimiert, erfüllen aber nicht die Sicherheitsansprüche von Unternehmen. Dem „Plug-and-Play"-Gedanken folgend, stellen Access Points an ihrer

**iX-TRACT**

- Unautorisierte WLANs sind zu einem der größten Risiken für Unternehmensnetze geworden.
- Das Suchen von Access Points per Funk („Warwalking") kommt wegen der geringen Präzision, des hohen Aufwands und rechtlicher Fallstricke selten in Betracht.
- Ethernet-basierte Verfahren sind effizient, präzise und flexibel. Sie können selbst in großen Netzen und in kurzen Intervallen nach „wilder" WLAN-Hardware suchen.

LAN-Schnittstelle einen DHCP-Client zur automatischen Integration in bestehende LANs bereit. Gleichzeitig bilden die APs für die über WLAN angeschlossenen Geräte ein eigenes Subnetz, das über Network Address Translation (NAT) ans Kabelnetz angebunden ist. Der Access Point dient hier als DHCP-Server für das Funknetzwerk.

Privat genutzte APs bieten in der Regel eine Web-Administrationsoberfläche an, sowohl über kabelgebundene als auch über kabellose Schnittstellen. Häufig sind diese Zugänge anfänglich nur mit einem Standardpasswort geschützt, das manchmal sogar auf der Login-Website steht. Einige Access-Point-Anbieter verzichten gänzlich auf einen initialen Passwortschutz.

In vielen Unternehmen müssen sich WLAN-Clients nur einseitig gegenüber dem Access Point authentifizieren. Eine Authentifizierung des AP gegenüber dem Client ist selten vorgesehen. Es ist also möglich, den Netzwerknamen (Service Set Identifier, SSID) eines unautorisierten Access Points derart zu wählen, dass er sich für technische Laien kaum von einem autorisierten Access Point unterscheidet – bis auf die Tatsache, dass das unautorisierte WLAN auch ohne Schlüsseleingabe funktioniert.

In Unternehmensnetzwerken sind Zugriffskontrollen auf Netzwerkebene die Ausnahme. Jede Person, die sich Zugang zu einem Ethernet-Segment verschaffen kann, hat direkten Zugriff auf das interne Netz. Verfahren, die dies verhindern sollen, etwa Network Access Control (NAC), haben sich aufgrund des hohen Implementierungsaufwands bisher nicht durchgesetzt.

Insgesamt führt die Installation ungesicherter WLANs dazu, dass sowohl der physische als auch der logische Perimeterschutz des Unternehmens unterlaufen werden. Angreifer sind so in der Lage, sich mit dem Unternehmensnetzwerk zu verbinden, ohne eine persönliche Zugangskontrolle oder eine Firewall überwinden zu müssen (siehe Abb. 2).

Weiterhin ist fraglich, in welcher Form mögliche Angreifer belangt werden können, da ein offenes WLAN nicht als „besonders gesichert“ gelten kann und es sich somit rein formal nicht von einem für die Öffentlichkeit bestimmten Hotspot-Service unterscheidet.

Nach Erfahrung der Autoren birgt von allen Gefahren, die von WLANs in einem Unternehmensnetzwerk ausgehen (WEP/WPA-Verschlüsselungsbruch, Man-in-the-Middle-Angriffe et cetera), das unautorisierte Installieren ungesicherter Access Points derzeit das höchste Risiko.

Für eine systematische Suche nach Funknetzen (Wardriving/-walking) wird ein Laptop mit WLAN-Empfänger, einer optionalen Antenne sowie entsprechender Scanner-Software, etwa Kismet oder Netstumbler, ausgestattet und das zu untersuchende Areal abgeschritten oder durchfahren. Warwalking kann auch falsch konfigurierte oder unternehmensfremde WLAN-Komponenten aufspüren. In Verbindung mit GPS-Hardware lässt sich so etwa eine Karte mit korrespondierenden Messergebnissen erstellen. Leider zeigt der Warwalking-Ansatz in der Praxis eine Reihe von Schwächen beim Aufspüren unautorisierter WLANs.

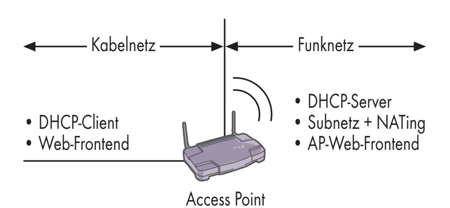
## Exakte Ortung von WLANs schwierig

Die Ausbreitung der Funkwellen wird stark von der baulichen Umgebung beeinflusst; Reflexions- und Dämpfungseffekte erschweren die Ortung oft erheblich. Insbesondere die verwendeten Baumaterialien bestimmen, wie sich die Funkwellen in dem für WLAN gängigen 2,4-GHz-Band verhalten. Aber auch Interferenzen mit anderen Funksendern oder elektrischen Geräten wirken sich auf den Bereich aus, in dem die Signale eines Access Point in ausreichender Qualität zu empfangen sind.

Daher gestaltet sich die exakte Ortung eines Access Point schwierig. Ohne umfangreiche Spezialausrüstung kann aber gerade in dicht bebauten Gebieten niemand ein WLAN-Signal auch nur dem eigenen Firmengelände zuordnen – geschweige denn den Access Point wirklich finden.

Besteht Unsicherheit darüber, ob ein WLAN-Signal seinen Ursprung im eigenen Firmengelände hat, ist dringend davon abzuraten, dieses WLAN einer intensiven Untersuchung, etwa einem Angriff auf den WEP-Schlüssel, zu unterziehen oder gar Methoden der „Active-Defense“ wie Störsender einzusetzen. Das bedroht nicht nur den nachbarschaftlichen Frieden. Man begibt sich auch rechtlich in unsicheres Fahrwasser. Nach der Novellierung des § 202c StGB ist schon der bloße Besitz geeigneter Cracking-Software strafbar.

Abseits dieser grundsätzlichen Hürden birgt die Praxis oft weitere Tücken. Allein die Größe des zu untersuchenden Areals, beispielsweise die Produktionsstätte eines Automobilherstellers, kann die Fitness des „Warwalker“ auf eine harte Probe stellen. Manchmal ist das Abschreiten des zu prüfenden Geländes, etwa auf Flughäfen oder in industriellen Produktionsbereichen, aufgrund strenger Sicherheitsvorschriften schlicht verboten. Häufig lassen Warwalkings Test-Installationen „auffliegen“, die gar nicht mit dem Unternehmensnetz verbunden sind und es daher gar nicht bedrohen.




**Funktionen von Access Points im LAN und WLAN (Abb. 1)**

Eine Methode für das Aufspüren unautorisierter WLANs sollte es also erlauben, „wilde“ Access Points physisch und logisch exakt zu lokalisieren sowie ihre Verbindung zum Unternehmensnetz zu verifizieren, wenig Präsenz vor Ort erfordern, sich weitgehend automatisieren lassen, dabei gleichzeitig ein möglichst geringes Störpotenzial für das Netzwerk und alle beteiligten Endgeräte aufweisen und keine fragwürdige Software im Sinne von § 202c StGB erfordern.

## LAN spürt WLANs auf

Einen solchen Ansatz haben die Autoren durch eine Ethernet-basierte Untersuchung des Netzwerks realisiert. Sie versucht, WLAN-Access-Points anhand von Merkmalen zu identifizieren, die sie auch dem kabelgebundenen Netz gegenüber offenbaren. Durch Einbeziehung mehrerer Faktoren lässt sich auf diese Weise eine Wahrscheinlichkeit dafür ermitteln, ob es sich um eine Hardwarekomponente handelt, die nicht zur unternehmenseigenen Infrastruktur gehört.

Für eine solche Untersuchung lassen sich gezielt Protokolle nutzen, die in den Unternehmen für die Netzadministration häufig ohnehin zum Einsatz kommen. Dadurch ist es meist möglich, auch weit verzweigte und entfernte Netzwerke ohne Firewall-Regelwerksänderungen in die Prüfung einzubeziehen.

Anders als bei gängiger Network-Discovery-Software, die auf ähnlichen Mechanismen basiert, liegt der Fokus

der Vorgehensweise nicht darauf, das komplette Netzinventar zu erstellen. Stattdessen soll eine intelligente Filterung den Aufwand bei der Identifizierung von Risikoträgern minimieren.

Als erster Indikator dient die Ethernet-seitige MAC-Adresse eines Access Point. Alle MAC-Adressen beginnen mit einem dem Hersteller des Geräts eindeutig zugewiesenen, 24-Bit langen Organizationally Unique Identifier (OUI). Eine Datenbank mit deren Zuordnung zu den jeweiligen Herstellern steht bei der IEEE öffentlich zur Verfügung (http://standards.ieee.org/regauth/oui/oui.txt).

Den Hardwaremarkt für Privatanwender bedienen im Allgemeinen andere Anbieter (oder zumindest andere Marken) als den für größere Organisationen. Die beschränken sich meist auch auf eine relativ kleine Anzahl von Lieferanten.

Da sich MAC-Adressen nur innerhalb eines Netzsegments direkt bestimmen lassen, sind weitere Hilfsmittel dafür nötig, Adressen der Geräte in anderen Segmenten zu sammeln. Hier bietet sich das Simple Network Management Protocol (SNMP) an. Daneben erhält man so den Switch-Port, an den ein verdächtiges Gerät angeschlossen ist, was das spätere Auffinden stark vereinfacht.

## Auf Entdeckungsreise

Man braucht für die Erfassung der physischen Adressen eine Liste der IP-Adressen aller Router und Switches zum gezielten Auslesen der ARP- oder CAM-Tabellen per SNMP. Diesen Schritt kann alternativ eine erweiterte Discovery-Phase ergänzen, die auf Ciscos Discovery Protocol (CDP) oder das Link Layer Discovery Protocol (LLDP) zurückgreift. So lassen sich SNMP-fähige Infrastrukturkomponenten selbstständig finden und abfragen, falls sie die entsprechenden Protokolle unterstützen.

Sämtliche ermittelten MAC-Adressen werden mit einer Whitelist von Hersteller-OUIs verglichen. Treffer gelten als unternehmenseigene, nicht weiter zu betrachtende Komponenten. Die Liste ist organisationsspezifisch und sollte nicht zu viele OUIs enthalten, um die Wahrscheinlichkeit dafür zu minimieren, dass ein „wilder“ AP unerkannt bleibt (False Positive).

Im nächsten Schritt sind die verbleibenden MAC-Adressen mit einer Blacklist der OUIs typischer Privatanwender-WLAN-Produkte abzugleichen. So lassen sich Geräte identifizieren, bei denen es sich mit hoher Wahrscheinlichkeit um unautorisierte WLAN-Hardware handelt.

Es sei nicht verschwiegen, dass auch ein MAC-basiertes Verfahren Schwächen aufweist. Manche Access Points bieten versierten Nutzern die Möglichkeit, die MAC-Adressen der Ethernet-Schnittstellen zu ändern. Voraussetzung dafür wäre aber neben der Expertise auch das Wissen, dass MAC-basierte Tests durchgeführt werden und wie die Whitelist aussieht. Außer bei gezielten Angriffen von Insidern dürfte diese Konstellation daher selten sein, ausschließen sollte man sie jedoch gerade deshalb nicht.

Auch bei sorgfältiger Zusammenstellung der White- und Blacklist taucht oft eine beträchtliche Anzahl von Geräten mit OUIs auf, die auf keiner der beiden Listen auftauchen. Weitere Heuristiken sind dafür nötig, die Wahrscheinlichkeit, ob es sich bei einem Gerät um einen AP handelt, abschätzen zu können.

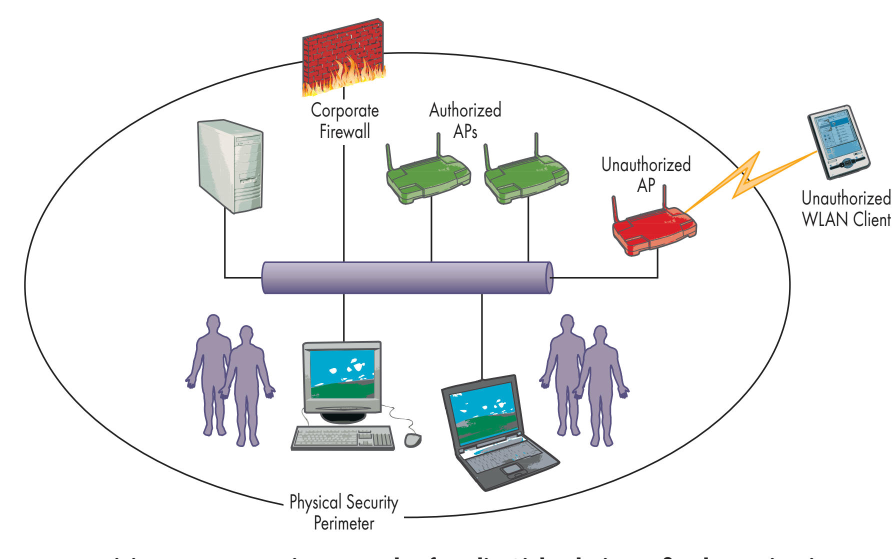
Zunächst kann eine SNMP-Anfrage der Einträge des „system“-Baums Anhaltspunkte für die Art des Geräts ergeben, insbesondere die zur Verfügung gestellten Services der Komponente sowie bestimmte Schlüsselwörter in der Systembeschreibung. Da sehr wenige Consumer-APs diese Funktion unterstützten, lässt sich auf diese Weise ein weiteres Kriterium erstellen.

Ein Netzwerkscanner liefert anschließend neben Informationen über offene Ports eine Einschätzung, welches Betriebssystem auf einem gescannten Host zum Einsatz kommt. Neben den verbreiteten Systemen wie Windows und Linux kann der Scanner mithilfe einer Fingerprint-Datenbank auch seltenere Systeme identifizieren. Die so ermittelten Bezeichner können wiederum auf Schlüsselbegriffe hin untersucht werden, was weitere Hinweise auf den Typ des untersuchten Hosts liefert. Auf vielen WLAN-Routern und Access Points laufen modifizierte Linux-Versionen, die einen typischen Fingerabdruck auf den IP-Paketen hinterlassen und somit direkt identifizierbar sind. Auch der Umkehrschluss ist möglich: Consumer-APs laufen nicht unter Windows, somit ist ein Windows-Fingerprint ein deutliches Zeichen dafür, dass es sich eben nicht um ein solches Gerät handelt.

## Auswerten mit Gewichtung

Des Weiteren kann der Scanner nach standardmäßig geöffneten Ports von Privatkunden-APs fahnden. Ist ein solcher offen, wird eine gezielte HTTP-Anfrage gestellt und die Antwort (sollte es eine geben) wieder nach den bereits erwähnten Schlüsselwörtern durchsucht. Interessant sind vor allem diejenigen TCP-Ports, die für das Web-Administrations-Interface, für Telefonie-Anwendungen oder sonstige herstellerspezifische Dienste geöffnet sind.

Die Ergebnisse sämtlicher Tests speichert eine Datenbank, verknüpft mit den entsprechenden Hosts. Das Auswerten erfolgt wie bei modernen Spam-Filtern: Jeder Indikator erhält eine Gewichtung, und für jeden Host mit verdächtiger MAC-Adresse ergibt sich ein Score. Wann immer auf einem Host ein Indikator positiv ist (etwa ein Schlüsselwort in der Beschreibung des OS-Fingerprints),




**Unautorisierte Access Points unterlaufen die Sicherheitsmaßnahmen in einem Unternehmensnetz (Abb. 2).**

erhöht er den Punktwert. Die Daten zu einzelnen Bewertungen bleiben erhalten, sodass man auch nach dem Scan-Lauf die Gewichtung dynamisch verändern kann.

Sind alle Merkmale ausgewertet, so lässt sich aus dem ermittelten Score der einzelnen Hosts eine absteigend sortierte Liste erstellen, an deren Anfang die wahrscheinlichsten Kandidaten für einen unautorisierten Access Point stehen. Sie kann zur Verdeutlichung Schwellenwerte anzeigen, die sich aus den Erfahrungen der letzten Scans ergeben haben. Auf diese Weise kann man drei Gruppen von Hosts bilden: diejenigen, die mit an Sicherheit grenzender Wahrscheinlichkeit Access Points sind, solche, die nur verdächtig erscheinen und eine verbleibende Gruppe relativ unauffälliger Hosts.

Die Ergebnisse zeigen die betroffenen IP- und MAC-Adressen, die Adresse des beteiligten Switch sowie dessen betroffenen Port. Als Standard-Ausgabeformat dienen HTML, CSV oder ASCII, anpassbar an die individuellen Anforderungen eines Unternehmens. Die Unterlagen der Prüfung sind so gestaltet, dass unabhängige Prüfer und Auditoren sie nachvollziehen und anerkennen können.

## Fazit

Der beschriebene Prozess kam bereits in einigen Organisationen zum Einsatz. Dank der Berücksichtigung mehrerer Faktoren erwies sich das Bewertungssystem als robust. Zudem lässt es sich je nach Gegebenheiten anpassen oder erweitern. Es hat sich gezeigt, dass das Verfahren – nach einem initialen Aufwand für das Einrichten und Anpassen der Black- und Whitelists sowie der weiteren Indikatoren – relativ wenig Aufwand erfordert, wie erwähnt die Voraussetzung für eine kontinuierliche Anwendung der Maßnahmen im operativen Betrieb.

In bisherigen Projekten lief der LAN-basierte WLAN-Scan in drei- bis sechsmonatigen Zyklen. Sollte es nötig sein, können besonders gefährdete Teile des Netzwerks auch in wesentlich kürzeren Abständen überprüft werden. Um den Installationsaufwand und Eingriffe in die Infrastruktur zu minimieren, sind die eingesetzten Werkzeuge auf einer Linux-Live-CD zusammengefasst, die sich bei Bedarf auf einer Festplatte installieren lässt.

Neben WLAN-APs kann das beschriebene Verfahren durch eine einfache Erweiterung der Black- und Whitelists auch andere unautorisierte Hardware, beispielsweise Switches, Drucker oder Laptops finden. Außerdem bietet es sich als Alternative zu präventiven Zugriffskontrollen auf Netzwerkebene an, die die Notwendigkeit aufwendiger Netzwerk-Zugriffskontrollen verringert. (un)


MARCEL KNOP

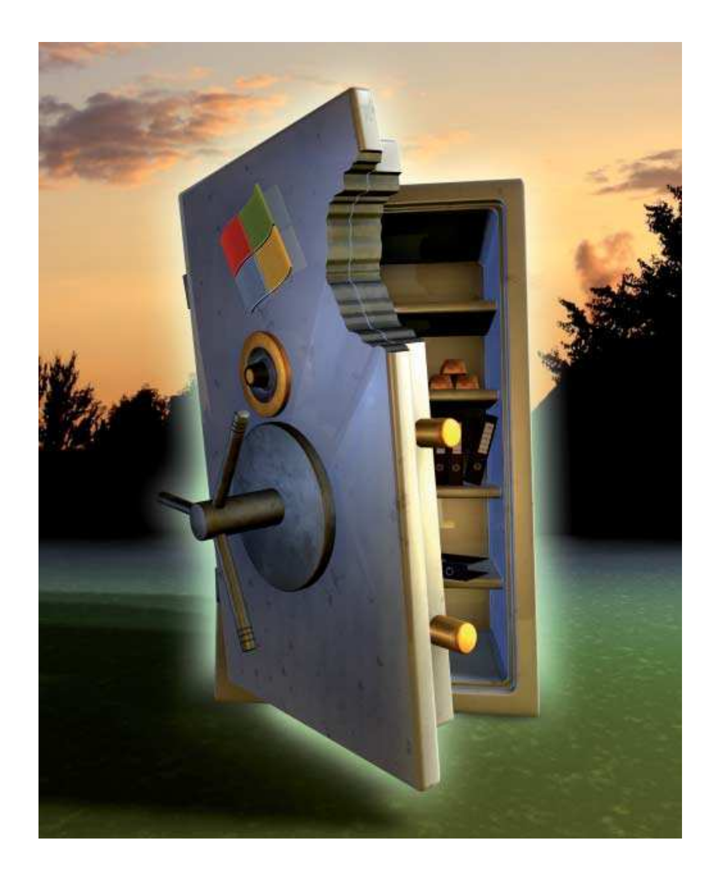
ist Engagement-Manager bei KPMG mit dem Schwerpunkt Prüfung und Beratung im Bereich IT-Sicherheit.

MICHAEL G. KAISER

ist freiberuflicher Softwareentwickler und Doktorand an der European Business School, Oestrich-Winkel.





Auch der Passport-Nachfolger Cardspace ist angreifbar

# Drei, zwei, eins ... weg

Christoph Löhr, Xuan Chen

Microsofts Cardspace soll die Benutzeranmeldung nicht nur einfacher, sondern auch sicherer machen als die herkömmliche Passwortabfrage. Die attraktivste Umsetzung des Konzepts mit einem Browser als Client könnte jedoch Angriffe wie Pharming ermöglichen.

Man muss nicht seine gesamte Freizeit im Internet verbringen, um eine große Menge an Benutzerkonten vorweisen zu können. Onlineeinkäufe wären ohne sie undenkbar, und die Registrierung bei Web-2.0-Angeboten bringt Vorteile wie Personalisierung. Die digitale Identität wird somit zu einem zentralen Bestandteil des Internet und gewinnt gleichzeitig an Attraktivität für Kriminelle. Die herkömmliche Authentifizierung mit Passwort gilt schon lange als unsicher; zahlreiche Missbrauchsfälle sind bekannt.

Mit Cardspace entwickelte Microsoft eine neue Identitätsverwaltung, die von den Schwächen seines Vorgängers „Passport“ frei sein sollte [1]. Das Verfahren vereinfacht die Verwaltung digitaler Identitäten, denn der Benutzer erstellt lediglich eine sogenannte Infocard mit seinen persönlichen Daten – eine Art Personalausweis für seine Onlinetätigkeit. Fordert eine Webseite zur Anmeldung auf, identifiziert er sich mit einem Klick auf seine Infocard. Die Eingabe eines Passworts oder anderer Identitätsinformationen auf der Seite ist nicht mehr nötig, da Cardspace sie durch ein kryptografisch gesichertes Token ersetzt. Microsoft führte Cardspace mit dem .Net Framework 3.0 ein. Es ist für Windows XP und 2003 Server nachrüstbar, Vista enthält es bereits. Für Firefox gibt es passende Plug-ins. Basierend auf offenen Standards wie WS-Security (siehe *iX*-Link) hat das neue Identitätssystem das Potenzial, die marode Authentifizierung per Passwort zu revolutionieren. Ähnliche Ansätze verfolgen die Projekte Liberty Alliance, OpenID und Higgins.

## Vier Parteien für eine Anmeldung

Das Cardspace-Protokoll verbindet vier Parteien, die während der Anmeldung kommunizieren: den Browser, die Relying Party, den Identity Selector und den Identity Provider. Der Identity Selector ist eine Browser-Erweiterung, die unter anderem zur Verwaltung der Identitäten dient – ähnlich wie ein Passwortmanager.

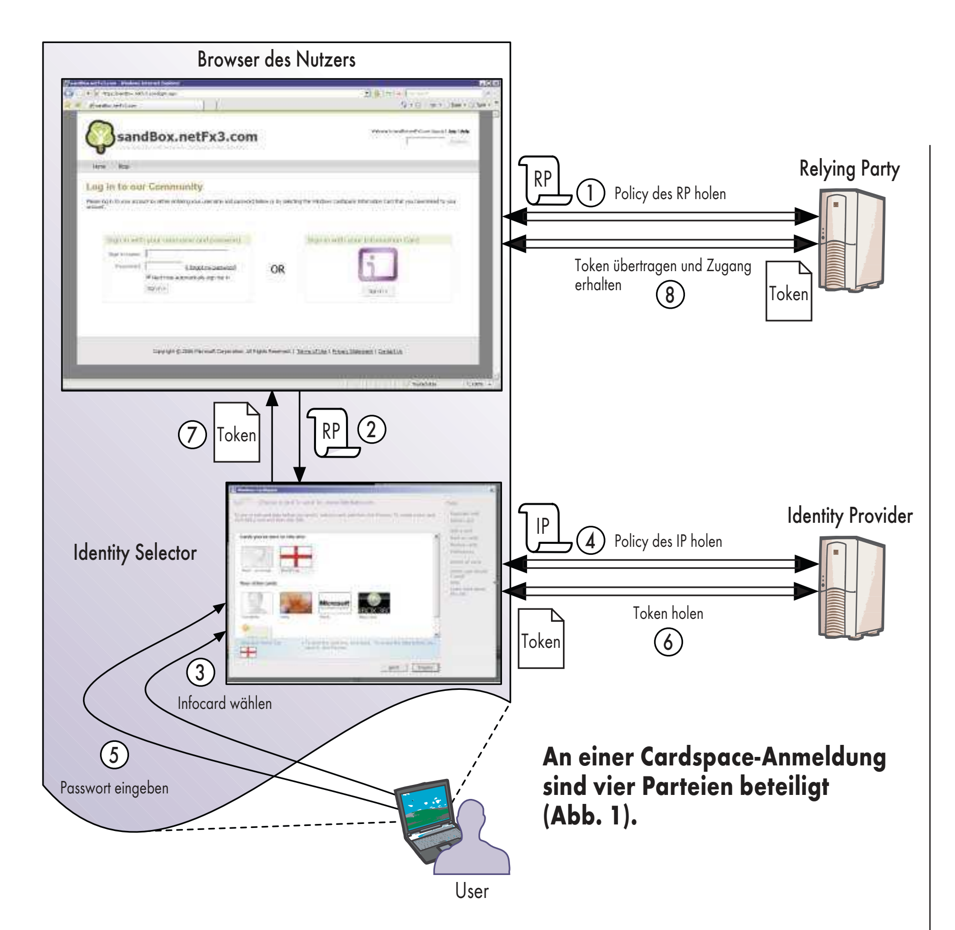
In der Praxis nimmt der Benutzer per Browser Kontakt zu einer Webseite (Relying Party) auf und fordert die Anmeldung per Cardspace an. Die Relying Party sendet daraufhin ihre Policy, die definiert, welche Informationen sie vom Benutzer wünscht (siehe Abb. 1). Hierbei kann sie festlegen, ob die Infocard von einer dritten Instanz stammen muss (Managed Card) oder eine vom Benutzer erstellte Identität ausreicht.

Diese Informationen leitet der Browser an den Identity Selector weiter. Dort wählt der Anwender die gewünschte Karte aus, und der Identity Selector nimmt Kontakt mit dem Identity Provider auf. Handelt es sich um eine selbst erstellte Infocard, ist dieser bereits Teil der Client-Software, andernfalls handelt es sich um einen vertrauenswürdigen dritten Server. Der Identity Provider sendet nun seine Policy, und der Benutzer muss sich gegebenenfalls dort authentifizieren. Dazu benutzt er ein Passwort, ein Zertifikat oder ein Kerberos-Ticket.

Die verschlüsselten Anmeldedaten (Token) übergibt der Identity Provider an den Identity Selector, der sie wiederum an den Browser weiterreicht. Die eigentliche Anmeldung schließt der Browser durch Senden des Tokens an die Relying Party ab. Nach erfolgreicher Prüfung dort ist der Benutzer angemeldet.

## Der Browser als Achillesferse

Bei diesem Verfahren kommuniziert die Relying Party niemals direkt, sondern nur über den Browser des Benutzers mit den einzelnen Teilnehmern des Cardspace-Systems. Sie weiß nicht, wie das Token entstanden ist und kann nur seine Gültigkeit überprüfen. Darin besteht die Achillesferse




**An einer Cardspace-Anmeldung sind vier Parteien beteiligt (Abb. 1).**

der Umsetzung der Technik via Browser: Er fungiert als Mediator des Tokens, ohne dabei in seinen Funktionen eingeschränkt zu sein. Allgemeine Attacken gegen den Browser lassen sich somit auf die Cardspace-Authentifizierung übertragen.

Cardspace will einen Angreifer daran hindern, in den Besitz des Tokens zu gelangen. Obwohl sich aus ihm keine Identitätsinformationen extrahieren lassen, kann man es für die Anmeldung im Namen des legitimen Nutzers verwenden und Zugang zu seinen Diensten erlangen. Um Zugriff auf das Token zu bekommen, muss der Angreifer die Same Origin Policy des Browsers umgehen. Sie bestimmt, ob ein Dokumentenobjekt auf eines aus einer anderen Quelle zugreifen darf. Stimmen Protokoll, Domain und Portnummer überein, gehören die Objekte zum selben Sicherheitskontext und dürfen miteinander kommunizieren. Gelingt es einem Angreifer, in den Sicherheitskontext der Relying Party zu gelangen, kann er Javascript-Code einbetten, der das Token abfängt.

Eine möglicher Weg dahin ist Cross-Site Scripting, das Lücken auf dem Server der Relying Party ausnutzt. Diese Attacken lassen sich jedoch nur gegen einzelne Relying Parties einsetzen. Eine andere Variante sind (dynamische) Pharming-Angriffe, bei denen der Angreifer die Namensauflösung verfälscht und von seinem eigenen Server bösen Javascript-Code holt, der auf das DOM-Modell des Nutzers zugreift. Da der Übeltäter im Normalfall seinen Code nicht direkt auf der Ziel-Webseite ablegen kann, muss er die Same Origin Policy aushebeln. Hierzu trägt er vor dem vorhandenen DNS-Eintrag der Relying Party die IP-Adresse seines eigenen Webservers ein. Ruft der Nutzer nun die URL des zu attackierenden Servers auf, landet er zuerst auf dem Rechner des Angreifers.

Hierbei entsteht jedoch eine neue Schwierigkeit: Der Angreifer möchte gleichzeitig Daten von zwei verschiedenen Servern laden. Der jetzige Aufbau nimmt aber nur Kontakt zu einem Server auf. Zwar sieht DNS eine Gültigkeitsdauer (Time-to-live) für Einträge vor, dies lässt sich jedoch hier nicht ausnutzen. Denn Browser ignorieren den Time-to-live-Wert, sie halten den DNS-Eintrag für eine selbstbestimmte Zeit im Cache. Beim Internet Explorer beträgt diese Zeit 30 Minuten, bei Firefox nur eine Minute. Währenddessen kann der Angreifer den Browser nicht zu einer zweiten DNS-Anfrage zwingen, die ihm eine andere Adresse für die Domain unterschieben würde.

## Wenn der falsche Server schweigt

Hierfür benötigt er den zweiten Eintrag der korrekten Adresse. Ist die erste nicht

erreichbar, nimmt der Browser mit dem zweiten Eintrag Kontakt auf. Um seinen Server nach dem Laden seines Codes unerreichbar zu machen, schaltet der Angreifer ihn einfach ab. Der Browser erreicht die erste IP-Adresse nun nicht mehr und weicht auf die zweite aus, die des echten Webservers, wo er die Anmeldeseite lädt. Dass DNS-Antworten sich fälschen lassen, belegen einige Meldungen der letzten Zeit (siehe *iX*-Link). Auch sind Drive-by-Pharming-Techniken [2], bei denen Webseiten Router-Konfigurationen manipulieren, oder kostenlose, aber trügerische öffentliche Hotspots leichter umzusetzende Angriffsmöglichkeiten.

Zusätzlich benötigt der Angreifer ein gültiges Zertifikat für seinen Server, das jedoch auf die Domain der attackierten Webseite ausgestellt sein muss. Zwar kam es in der Praxis mehrfach vor, dass im Browser festverdrahtete Zertifizierungsinstanzen den falschen Personen Zertifikate ausgehändigt haben. Dabei handelte es sich jedoch um Einzelfälle. Daher muss der Übeltäter ein selbst erstelltes Zertifikat verwenden. Alternativ kann er versuchen, den Benutzer zur Installation seines Root-CA-Zertifikats zu überreden. Ist eine dieser Bedingungen erfüllt, hat der Angriff Erfolg – wenn der Bedrohte das falsche Zertifikat akzeptiert.

Schlecht stehen die Chance dafür nicht. Denn der durchschnittliche Internetnutzer vermag nicht, die Echtheit eines Servers anhand eines SSL-Zertifikats zu erkennen. Dies belegen Nutzerstudien [3, 4], deren Ergebnis die massive Zahl der Phishing-Angriffe belegt. Folglich reduziert sich die Sicherheit einer Cardspace-Authentifizierung auf die der klassischen Passwortabfrage. Eine Demonstration gibt es im Web [a].

Der hier beschriebene Angriff ist möglich, weil einzig und allein die Same Origin Policy des Browers das Versenden des Tokens kontrolliert. Gelingt es, diese Hürde durch Änderungen am Domain-Eintrag zu überwinden, erlaubt die Software Zugriff auf das Cardspace-Token unter anderem per Javascript.

## Mehr Sicherheit durch ein Verbot

Mehr Sicherheit brächte es, den Browsern den DOM-Zugriff auf das Token-Objekt zu verbieten, etwa durch Deklaration als privat. Das schützt seinen Inhalt vor dem Zugriff durch Skriptsprachen, während der Browser es für die Anmeldung bereithalten kann. Für das Funktionieren von Webseiten ist der Zugriff auf dieses Datenobjekt irrelevant, da es nur für die Cardspace-Anmeldung Bedeutung hat. Einen vergleichbaren Isolationsmechanismus hat Microsoft bereits für Cookies umgesetzt. So verhindert der Internet Explorer 6 (SP1) das Auslesen eines Cookie durch Javascript bei im HTTP-Header gesetzter „HTTPOnly“-Direktive [b].

Während Änderungen am Browser den beschriebenen Angriff unterbinden können, beheben sie nicht die Schwäche des Cardspace-Protokolls, die die Nutzung des gestohlenen Tokens überhaupt erlaubt. Der Angreifer benutzt dazu einen sogenannten Replay-Angriff: Er schickt dem Server zuvor mitgeschnittene verschlüsselte Daten, beispielsweise Namen und Passwort. Der Server entschlüsselt die Daten und meldet den Angreifer an.

Die Entwickler haben diese Art des Angriffs anscheinend nicht bedacht und generieren das Token verbindungsunabhängig. Diese Schwachstelle im Design des Protokolls macht das Verfahren für klassische Man-in-the-Middle-Angriffe verwundbar. Abhilfe schaffte es, das Token kryptografisch an die Verbindung zwischen Browser und Relying Party zu binden. Das stellt sicher, dass die Relying Party ein Token erhält, das tatsächlich von dem Rechner stammt, der sich anfangs auf die Login-Seite begeben hat. Bewerkstelligen lässt sich diese Zuordnung mit einem im Token enthaltenen Fingerprint.

## Fazit

Microsofts Cardspace bietet Potenzial zur Verbesserung der Nutzerauthentifizierung und zum Schutz vor Identitätsdiebstahl. Zudem enthält es signifikante Verbesserungen gegenüber dem gescheiterten Passport. Das Protokoll scheint solide zu sein, einzig die Kombination des Metasystems mit dem Browser und anderen Systemkomponenten öffnet es für Angriffe. Hier liegt die Schwäche der Same Origin Policy.

Es sind Angriffe denkbar, die der Nutzer nicht erkennt. So leiten viele Hotspots standardmäßig den Kunden bei Anwahl einer beliebigen Webseite auf die Login-Seite ihres Betreibers um. In diesen Prozess kann man das Herunterladen eines Wurzelzertifikats integrieren, ohne dass ein Zusammenhang mit Cardspace erkennbar wäre.

Sicherheit ist eine Verkettung von Teilsystemen, deren isolierte Betrachtung nicht hinreicht. Nur ihr Zusammenspiel entfaltet Wirkung. Zudem muss ein innovatives Identitätsmanagement Robustheit auch bei exotischen Angriffen gewährleisten. Für den durchschnittlichen Benutzer, der Browser-Warnungen ignoriert, bringt Cardspace deshalb weder mehr noch weniger Sicherheit als das klassische Passwort. (ck)

### Onlinequellen

[a] On the Insecurity of Microsoft’s Identity-Metasystem CardSpace http://demo.nds.rub.de/cardspace

[b] Cookies mit „HTTPonly“ schützen http://msdn.microsoft.com/en-us/library/ms533046.aspx

CHRISTOPH LÖHR UND XUAN CHEN

sind Master-Studenten am Horst-Görtz Institut für IT-Sicherheit der Ruhr-Universität Bochum. Die vorgestellten Ergebnisse basieren auf der Abschlussarbeit von Chen. Christoph war für die Implementierung zuständig.

### Literatur

[1] D. Kormann, A. Rubin; Risks of the Passport signon protocol; Computer Networks 2000, Vol. 33, p. 51-58

[2] Sid Stamm, Zulfikar Ramzan, Markus Jakobsson; Drive-By Pharming, in: ICICS 2007, p. 495-506

[3] Rachna Dhamija, J. D. Tygar, Marti A. Hearst; Why phishing works, in: CHI (ACM); 2006, p. 581-590

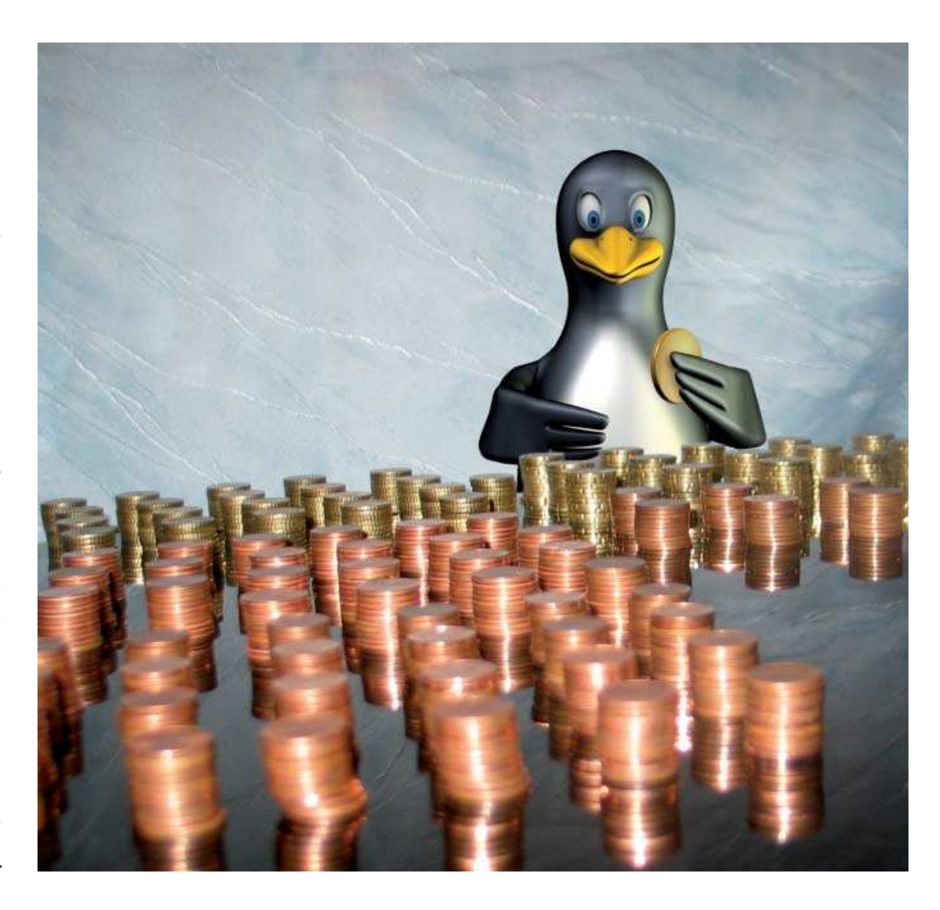
[4] Stuart Schechter, Rachna Dhamija, Andy Ozment, Ian Fischer; The Emperor’s New Security Indicators, in: Symposium on Security and Privacy (IEEE) 2007, p. 51-65

[5] Chris Karlos, Umesh Shankar, J. D. Tygar, David Wagner; Dynamic pharming attacks and locked same-origin policies for web browsers, in: CCS ’07: Proceedings of the 14th ACM conference on Computer and communications security, p. 58-71

[6] Tina Müller; Websicherheit; Cross-Site Request Forgery verhindern, Mein Cookie gehört mir; *iX* 6/08, S. 143





Open Source und Business: Ein Widerspruch in sich?

# Freie Marktmacht

Rüdiger Berlich

Würde ein Versandhaus seine Waren verschenken, statt sie mit Gewinn zu verkaufen, wäre es innerhalb kürzester Zeit bankrott. Im Bereich der Software hat sich jedoch ein Geschäftsmodell etabliert, das genau dies – das überwiegende Verschenken der eigenen Produkte – zum Prinzip erhebt.

Open Source und Business scheinen auf den ersten Blick einen inhärenten Widerspruch darzustellen. Wer die einschlägigen Pressemeldungen verfolgt, weiß jedoch, dass dem nicht so ist. Dieser Artikel soll die Hintergründe wirtschaftlicher Tätigkeit im Bereich von Open-Source-Software (OSS) beleuchten.

Besonders in den letzten Monaten scheint das OSS-Geschäftsmodell einen erheblichen Aufschwung zu erleben. Die Pressemeldungen zeichnen ein eindeutiges Bild: MySQL geht für eine Milliarde Dollar über den Ladentisch, Trolltech erzielt beim Verkauf an Nokia vergleichsweise magere 105 Millionen Euro. Dafür verkauft Asus auf Anhieb 300 000 EeePCs mit Linux, und Red Hat feiert einen Umsatzrekord nach dem anderen (siehe Abb. 1).

Das Marktforschungsunternehmen IDC zeigt, dass das Businessmodell „Open Source“ nicht nur aus dem gewinnbringenden Verkauf der Firma besteht. Für 2006 nennt es die Zahl von 1,8 Milliarden Dollar Umsatz mit „Standalone Open Source Software“ und prognostiziert ein Wachstum auf 5,8 Milliarden bis 2011 (siehe Onlinequellen [a]). Ganz klar, das Geschäft mit und um freie Software boomt.

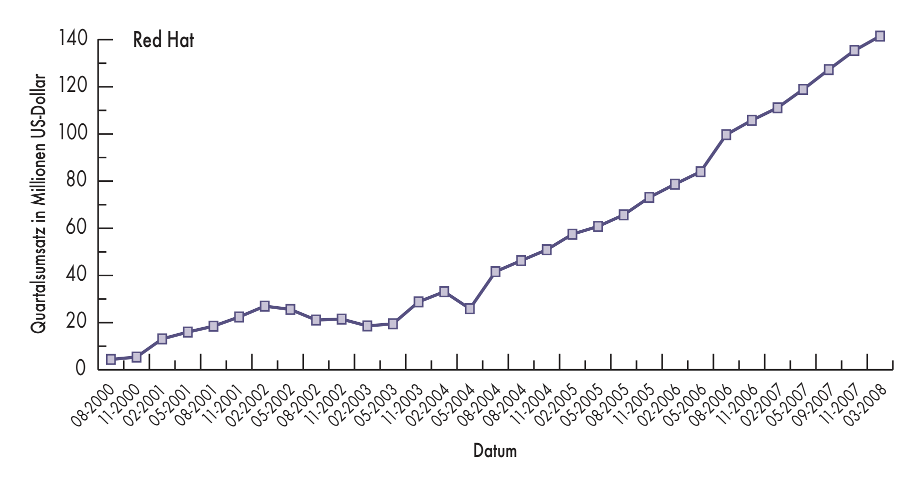
## Ein nicht ganz neues Phänomen

Ganz neu ist diese Tatsache allerdings nicht. Linux-Distributoren wie Red Hat, Suse (heute Novell) oder Mandrake (heute Mandriva) etablierten sich schon in den neunziger Jahren als Hauptvertreter dieses Marktes. Ihr Kerngeschäft umfasste zu diesem Zeitpunkt Zusammenstellungen frei verfügbarer Programme und Software-Bibliotheken rund um das Betriebssystem Linux. Versehen mit einfachen Installationsroutinen, Handbüchern und technischem Support erhielt der Kunde gegenüber den frei über die damals noch sehr langsame Netzverbindungen verfügbaren Einzelkomponenten einen deutlichen Mehrwert.

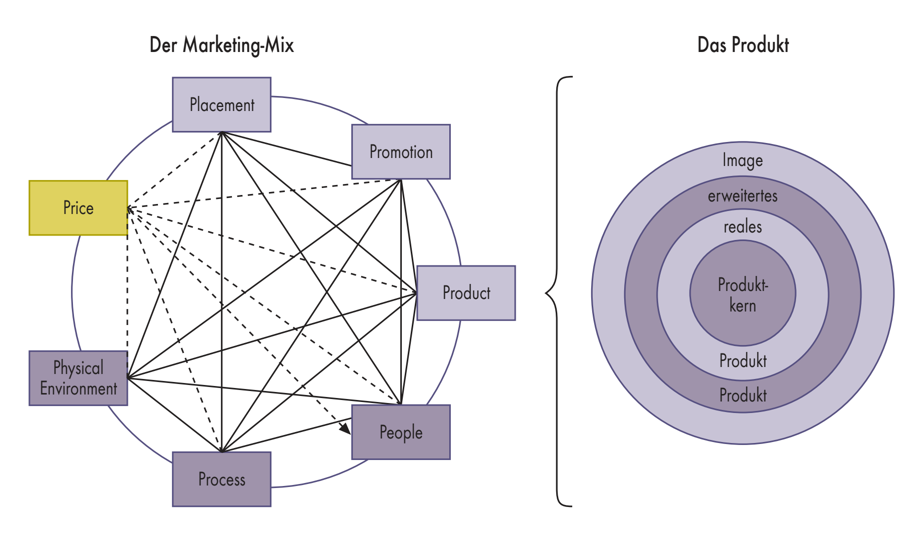
Zumeist war es zudem explizit erlaubt, die Produkte auf einer beliebigen Anzahl von Rechnern zu installieren, ohne allerdings – ohne weiteres finanzielles Engagement – für alle diese Rechner auch technische Unterstützung in Anspruch nehmen zu können. So wurde der Mehrwert nicht mit einer Einschränkung erkauft. Der Dämpfungsfaktor im Geschäft der Distributoren durch eine fehlende Realisierung potenzieller Verkäufe (schließlich konnte ein Kunde das Produkt auch legal von einem Bekannten kopieren) schien sich nicht gravierend auszuwirken. Hierzu hat sicherlich beigetragen, dass – anders als heute – das Verbreitungsmedium Internet aufgrund zu geringer Netzwerkbandbreite ausschied.

Jedoch konnten die Linux-Distributoren durchaus von der kostenlosen Arbeitskraft der Urheber der jeweiligen Softwarekomponenten profitieren. Neben Enthusiasten finden sich unter diesen häufig auch Mitarbeiter von Firmen, die ihre Produkte unter einer Open-Source-Lizenz freigeben. Die Qualität der entwickelten Software entspricht durchaus kommerziellen Maßstäben.

Man könnte sogar noch weiter zurückgehen, hin zu den OSS-Urvätern (Mütter gab es damals wie heute leider nur wenige). Sie dürften sich zu Beginn weniger über ihre Software als über die




**Red Hats Erfolg mit seiner Open-Source-Strategie zeigt sich auch in der seit Jahren steil nach oben zeigenden Kurve der Umsatzzahlen [b] (Abb. 1).**




**Beim Interesse für Open-Source-Produkte dürfte das Produkt-Image – eines der sieben englischen „P“s des Marketings – eine größere Rolle spielen als das bei proprietären Produkten der Fall ist (Abb. 2).**

Zugehörigkeit zum elitären Zirkel der ersten Computernutzer definiert haben. Zu Helden der Neuzeit wurden sie eher unfreiwillig, weil in den späten 70er- und frühen 80er-Jahren die Selbstverständlichkeit, Software „einfach nutzen zu können“ und gemeinsam an Features und Bugfixes zu arbeiten, mit zunehmender Verbreitung von Computern dem Business Modell „Lizenzverkauf“ wich. Damit einher ging eine Abschottung der Computerfirmen untereinander – die Unix-Geschichte ist Zeugnis genug für diese Entwicklung. Gleichzeitig versuchten Leute wie Richard Stallman, die sterbende Kultur des freien Austauschs von Software zu erhalten.

Etwas überspitzt könnte man sagen, dass auch die Geschichte des Open-Source-Business zu dieser Zeit beginnt. Denn Stallman – Autor des einzig wahren Editors Emacs und Initiator der GNU General Public License – finanzierte seine Free Software Foundation zu Beginn nicht zuletzt durch den Verkauf von Tapes mit freier Software. 150 Dollar kostete ein Band mit Emacs, durchaus kein kleiner Betrag [1]. Im Grunde nahm Stallman damit schon das Modell vorweg, mit dem die meisten kommerziellen Linux-Distributionen groß geworden sind.

**iX-TRACT**

- Kommerzielle Aktivitäten tragen signifikant zum Erfolg von Open-Source-Software bei.
- Sieben Ps beschreiben im Englischen die zentralen Aspekte, wie ein Produkt in den Markt gelangt.
- Ohne eine funktionierende Community sind Ansätze zum „Going Open Source“ meist zum Scheitern verurteilt.

## Ein bisschen Marketingtheorie

Wie schon die IDC-Studie andeutet, scheint heute auch das Geschäft mit einzelnen OSS-Anwendungen deutlich auf dem Wachstumspfad zu sein. Firmen, die eine Software unter einer Open-Source-Lizenz veröffentlichen wollen, können deshalb von etablierten Geschäftsmustern profitieren. Der weitere Artikel soll diese nun näher beleuchten und geht von einer Firma aus, die erstmals ein Softwareprodukt unter eine OSS-Lizenz stellen möchte.

Den theoretischen Hintergrund der Diskussion sollen einige Einstufungen liefern, wie sie häufig in wirtschaftlich motivierten Diskussionen auftauchen (Bild 2, vgl. auch [2]). Demnach umfasst jedes Produkt wenigstens drei Unterkategorien – den Kern (also etwa die Funktion „Texte schreiben“ in einer Textverarbeitung), das Äußere (Verpackung, Funktionsumfang, hier beispielsweise das Benutzer-Interface, Marke und Qualität) und das Image, also die Wahrnehmung durch die Öffentlichkeit. Je nach Produkt können hierzu noch ergänzende Faktoren wie Dienstleistungen (Support und Consulting, Sicherheitsupdates, …) kommen. Sie tragen natürlich zum Image des Produkts bei.

Ein Open-Source-Erzeugnis unterliegt hier also denselben Einstufungen wie jedes andere – auch eine elektrische Zahnbürste lässt sich so einordnen. Das Image eines OSS-Produkts (und der Firma, die es vertreibt) dürfte im Regelfall allerdings eine höhere Rolle spielen als bei dieser …

Auf der Ebene von Produktkern und Produktäußerem unterscheiden sich Open-Source- und proprietäre Produkte insbesondere durch die Anpassbarkeit – der Kunde ist nicht auf das Wohlwollen des Herstellers angewiesen. Eine Zahnbürste lässt sich zwar vielleicht mit etwas Geschick zu höheren Schwingzahlen animieren. Es ist aber eher unwahrscheinlich, dass diese hausgemach-

ten Änderungen Eingang in die nächste Release finden. Bei OSS ist dies jedoch Teil des Konzepts (auch wenn Änderungen, etwa am Linux-Kernel, durchaus einer strengen Kontrolle unterliegen).

## 7 Ps als Basis für Produkteinstufungen

Bei der Platzierung eines Produktes im Markt spielen aber noch weitere Faktoren eine Rolle – man spricht von den vier respektive sieben Ps. Um diese gebräuchliche Einstufung nicht zu durchbrechen, sind die Begriffe in Bild 2 im englischen Original wiedergegeben.

Neben den diskutierten Unterkategorien eines Produkts tragen drei weitere Faktoren wesentlich zum kommerziellen Erfolg bei: der Preis (Price), das Verteilungssystem (Placement) sowie die Art der Bekanntmachung (Promotion).

Signifikantestes Unterscheidungsmerkmal zwischen Open Source und herkömmlichen Produkten ist hier der Preis. Für Letztere gilt er als wichtigstes Regelinstrument für die Platzierung im Markt. Ein reines Softwareprojekt unter einer Open-Source-Lizenz ist aber für jedermann meist kostenlos verfügbar. Insofern man nicht mit dem Hersteller einer proprietären Software konkurriert, spielt bei OSS-Produkten der Preis als Regelinstrument also keine Rolle.

Lizenzumsätze lassen sich gleichwohl generieren. Eine übliche Strategie ist hier das Dual Licensing; die Software ist dabei unter einer viralen OSS-Lizenz – beispielsweise der GPL – sowie unter einer kommerziellen Lizenz verfügbar. Der Diskriminator zwischen kommerzieller und freier Nutzung stellt hier die Gefahr dar, eigene Produkte mit der Open-Source-Lizenz gewissermaßen zu „infizieren“. Sie müsste unter gewissen Umständen fortan etwa unter der freien Lizenz vertrieben werden. Da dies von den Nutzern der freien Software meist nicht gewünscht ist, erwerben sie lieber eine kommerzielle Lizenz. Sie stellt sie von diesen Verpflichtungen frei.

Auch „Placement“ und „Promotion“ gestalten sich bei freier Software anders. Der Kunde kann OSS einfach ausprobieren und im Zweifelsfall wieder wegschmeißen. Die Zugänglichkeit ist also eine ganz andere. Eine gute freie Software vermarktet sich deshalb teilweise von selbst.

Ein anderer Weg hin zu Lizenzumsätzen ist die Bereitstellung von kostenpflichtigen Zusatzprodukten, oder das Bundling mit Dienstleistungen (Support, Consulting, kostenpflichtige Updates, …). In diesem Fall kommen drei weitere „Ps“ hinzu: People (wer erbringt die Leistung?), Process (wie wird die Leistung erbracht?) und Physical Environment (Umfeld und Ambiente der Dienstleistung – wichtig beispielsweise beim Training).

## Unterscheidung durch Ausprägungen

Hier gibt es nur wenige Unterschiede zwischen herkömmlichen und Open-Source-Produkten. Gleichwohl bietet praktisch jeder OSS-Hersteller auch Dienstleistungen an. Dies geschieht nicht zuletzt deshalb, weil es ein einfaches Mittel ist, den geringeren Lizenzumsätzen entgegenzuwirken. Denn die Höhe der Dienstleistungsumsätze skaliert besonders mit der Menge der Produkte, die im Markt platziert werden konnten. Bei OSS ist diese oft höher als bei proprietären Produkten, denn zumindest das Basisprodukt ist ja in der Regel kostenlos. Und wer beispielsweise seine Firewall unter Linux mit kostenlosen Werkzeugen wie *iptables, ebtables oder arptables* einrichtet, dürfte gleichwohl häufig externe Hilfe benötigen.

Zudem lassen sich aufgrund der freien Verfügbarkeit Dienstleistungskategorien (zum Beispiel Portierung, Anpassung) finden, die bei proprietären Produkten weit weniger ausgeprägt sind.

An dieser Stelle sollte klar geworden sein, dass ein auf Open Source

### Univention – Open Source als Schlüsselstrategie

Die seit sieben Jahren am Markt befindliche Univention GmbH bietet mit „Univention Corporate Server“ (UCS) eine auf Debian GNU/Linux basierende Linux-Distribution an. Besonderes Merkmal dieser von dem Bremer Unternehmen auch als Linux-Komplettlösung vermarkteten Distribution ist ein am ehesten mit Active Directory oder Novell eDirectory vergleichbares Identity- und Infrastrukturmanagementsystem. Es fügt viele bekannte Open-Source-Pakete wie OpenLDAP, Heimdal Kerberos, OpenSSL oder Samba zu einer zentralen Managementplattform zusammen, die sich nicht nur zur Administration einzelner Server, sondern auch für anspruchsvolle, verteilte und heterogene Netze nutzen lassen.

Viele Anwender des Systems sehen UCS in erster Linie als Windows-Alternative und zwar sowohl für den Server- als auch für den Client-Bereich. In dieser Rolle setzen das System Bundes- und Landesbehörden, Kommunen, Banken und viele Mittelständler in Deutschland und im deutschsprachigen Ausland ein. Univention kündigte im Sommer 2006 die vollständige Lizenzierung aller in UCS und den darauf basierenden Produkten enthaltenen Eigenentwicklungen unter der GNU GPL an. Zuvor waren die Eigenentwicklungen proprietär und ließen sich erst nach Ablauf eines bestimmten Zeitintervalls unter den Bedingungen der GPL verwenden.

In Vertrieb und Marketing entstand dadurch das Problem, dass man zwar einerseits mit der Flexibilität und strategischen Sicherheit von Open-Source-Software warb, sich andererseits aber fragen lassen musste, was an dieser proprietären Software besser war als beispielsweise an der von Microsoft oder Novell. Trotzdem ging der Entscheidung intern eine intensive Diskussion und der Umsetzung dann eine halbjährige Review-Phase für den Quellcode voraus. Nicht zuletzt steigerte sich dadurch auch die Qualität der Software. Seit Ende 2006 stehen alle Univention-Quellcodes allgemein zum Download zur Verfügung. Unternehmen und Behörden, die die Software professionell einsetzen, greifen dennoch zur weiterhin verfügbaren kostenpflichtigen Lizenz. Diese ist Voraussetzung für den Bezug von Support- und Software-Maintenance im Rahmen bestimmter Standardverträge. Und gerade auf die Programmwartung können professionelle Anwender bei einem System wie UCS in der Regel nicht verzichten.

Für Univention war die Open-Source-Lizenzierung ein voller Erfolg. Während sich Umsatz und Gewinn in den ersten Jahren nur schleppend entwickelten, profitiert das Unternehmen in Folge der Open-Source-Lizenzierung nun von jährlichen Zuwachsraten von 25 bis 30 %. Zu diesem Erfolg mag auch der Zuwachs an Glaubwürdigkeit beitragen – Univention kann seinen Kunden nun von Anfang an alle Vorteile von OSS bieten. Und selbst vor einem kommerziell vertriebenen Nachbau der Software auf Basis der von Univention veröffentlichen Quellcodes besteht keine Angst. Denn dem Markt würde dies nur zeigen: Das Produkt ist so gut, dass andere es nachbauen. Dies würde sicherlich eher in mehr als weniger Kunden resultieren.

*Peter Ganten, Univention-Gründer und -Geschäftsführer*

## OTRS – ein erfolgreiches OSS-Business

Im Jahr 2001 startete das Open-Source-Projekt OTRS (www.otrs.org) als Ticket-System mit dem Ziel, ein flexibles und ergebnisorientiertes Tool für den Helpdesk bereitzustellen. Mittlerweile hat es sich darüber hinaus zu einem „Service Management Tool“ entwickelt und wird weltweit mit über 55 000 Installationen in großen wie in kleinen Firmen eingesetzt.

OSS im Firmeneinsatz braucht zwingend einen kompetenten Beratungspartner, schließlich müssen Firmen ihre Investitionen sichern und Projekterfolge langfristig gewährleisten. Unter dieser Prämisse erfolgte 2003 die Gründung der OTRS GmbH (www.otrs.com).

Trotz voller Auftragsbücher musste OTRS Anfangsschwierigkeiten überwinden und stand Anfang 2005 sogar fast vor dem Bankrott. Dank neuer Leitung erzielt das Unternehmen heute aber durchweg positive Betriebsergebnisse, und das bei einem jährlichen Mitarbeiter- und Umsatzwachstum von über 80 %. Seit 2007 firmiert OTRS als Aktiengesellschaft.

So sichert das OSS-Geschäftsmodell der OTRS AG das Einkommen von über 25 Mitarbeitern. Ein internationales Partnerprogramm und die Gründung der OTRS Inc. in Cupertino (Silicon Valley, USA) sind Ausdruck der Expansionsstrategie. Die Finanzierung des bisherigen Erfolgs basiert dabei auf einem gesunden organischen Wachstum aus dem eigenen Cash-Flow. Auf Venture Capital (VC) verzichtete OTRS bislang bewusst. Schlagworte wie „burn rate“ sind im Unternehmen unüblich.

Für den Erfolg der Firma ist die „Idee“ nur ein kleiner Faktor. Wichtiger ist das Team, das sich zusammenfindet. Die klare Erkennung des Problems, das man mit seiner Software lösen will, reicht am Anfang als technische Marschrichtung schon aus. Dass man wirklich gute Entwickler braucht, um ein neues Projekt aus dem Boden zu stampfen, versteht sich von selbst. Ebenfalls von zentraler Bedeutung ist es, von Anfang an auf den kaufmännischen Teil zu achten. Einen guten Kaufmann an Bord zu haben ist essenziell. Ohne ihn lässt sich keine Firma wirklich steuern.

Generell muss das Unternehmen auf maximale Offenheit ausgerichtet sein. Wer sein Projekt in Bewegung hält, braucht keine Angst zu haben, andere würden das Business wegnehmen. Ein erfolgreiches OSS-Business hilft seinen Multiplikatoren, statt seinen Konkurrenten Knüppel zwischen die Beine zu werfen.

Im OSS Business ist das im proprietären Umfeld übliche „Information Hiding“ Gift. Wer versucht, sein Expertenwissen zu hüten (intern oder extern), dürfte es nicht schaffen, eine produktive und kompetente Community aufzubauen. Und nur zusammen mit einer funktionierenden Community kann man seine Software in die Richtung entwickeln, die „der Markt“ braucht.

In einer OSS-Firma zu arbeiten, bedeutet Aufbau eines persönlichen Know-how-Kapitals, das sich ohne Einschränkungen bei zukünftigen Arbeitgebern einsetzen lässt. Dies gilt sowohl für Firmengründer als auch für Angestellte. Selbst wenn die Firma „mal den Bach runtergeht“: Wird das Programm „draußen“ eingesetzt, findet sich immer Arbeit.

Und der wichtigste Grund für ein OSS-Business: Wir sind die Guten! ;-)

*Burchard Steinbild, Co-Founder OTRS AG, OpenSLX GmbH & SuSE AG*

aufgebautes Geschäftsmodell denselben Marktgesetzen folgen muss wie jedes andere Business. Lediglich die Ausprägungen einzelner Komponenten sind anders.

Auffällig ist allerdings, dass reine Open-Source-Firmen bislang selten mehr als einige Hundert Mitarbeiter besitzen. Im Vergleich arbeiten bei Microsoft knapp 80 000 Mitarbeiter, IBM hat die 100 000er-Grenze lange hinter sich gelassen.

Hier spielt aber auch der (in diesem Artikel sonst nicht behandelte) Aspekt von Open Source als „Business Enabler“ hinein. Firmen wie IBM machen signifikante Umsätze auf der Basis von OSS (etwa im Clustering Bereich, oder als Betriebssystem für Mainframes), ohne sie direkt zu vermarkten. Bei entsprechenden Umsätzen steht der Aspekt „Open Source“ also nicht im Vordergrund. Ohne diesen wären die Umsätze aber oft nicht möglich.

Auch Firmen wie Microsoft profitieren indirekt von der Verfügbarkeit von OSS. Zum Beweis dieser These muss man sich nur einmal die Menge frei verfügbarer Windows-Programme unter www.sourceforge.net anschauen. Bei Apple wäre etwa Safari zu nennen, das letztendlich auf die KHTML-Engine zurückgeht.

## Vom Goldesel und dem armen Hund

Eine andere Einstufung von Produkten ist die ursprünglich von der Boston Consulting Group stammende Produktportfolio-Matrix. Hier ordnet man alle Produkte anhand der Kategorien „Relativer Marktanteil“ und „Marktwachstum“ an. Im Regelfall beginnt ein Produkt sein Leben bei hohem Marktwachstum und niedrigem Marktanteil (man bezeichnet es dann als „Fragezeichen“). Es entwickelt sich als Nächstes zum „Star“ (hohes Wachstum, hoher Marktanteil) und schließlich zur Cash Cow (niedriges Wachstum, hoher Marktanteil). In diesem Stadium schöpft der Hersteller die Gewinne ab. Nach einer (idealerweise langen) Zeit mutiert es zum „Armen Hund“ (niedriges Wachstum, niedriger Marktanteil), und das Unternehmen dürfte versuchen, das Produkt zu liquidieren.

Hier sei nun die These aufgestellt, dass die meisten Veröffentlichungen einer von der Anlage her proprietären Software als Open Source in die Phasen „Fragezeichen“ und „Armer Hund“ fallen, oder dass die Umwandlung zur Cash Cow nicht funktioniert hat.

Produkte in der Cash-Cow-Phase finanzieren oft andere Produkte mit, die noch in der Entwicklung stecken. Dem Risiko einer fehlgeschlagenen Veröffentlichung als Open Source dürften sich in dieser Phase nur wenige Unternehmen aussetzen.

Im Falle des „Armen Hunds“ oder der misslungenen Umwandlung bietet sich die Chance, mit dem Produkt auf andere Weise (und weitestgehend kostenneutral) noch einmal Geld zu verdienen. Und selbst, wenn dies nicht gelingt, kann man ja vielleicht einen Konkurrenten, dessen Produkt noch oder schon in der Cash-Cow-Phase steckt, ein wenig ärgern – seine Umsätze dürften vermutlich zurückgehen.

Anders sieht es in der „Fragezeichen“-Phase aus. Mit dem nachweisbaren Markterfolg von Open-Source-Produkten werden viele Firmen heute eine Open-Source-Strategie für ein neues Produkt zumindest diskutieren.

## Der Weg zur Open-Source-Software

Da stellt sich die Frage, welche Vorteile eine Open-Source-Strategie einer Firma bietet. Imagefaktoren können sicherlich nur bei wirklich großen Firmen dominieren. Vielmehr muss eine solche Entscheidung einen klaren Wirtschaftsvorsprung versprechen.

Zunächst einmal ist die hohe Verbreitung zu nennen, die höhere Umsätze außerhalb des Lizenzgeschäfts ermöglichen. Eine wichtige Rolle dürfte auch die Entwicklung der Marketingkosten für Softwareprodukte spielen. Die Kosten großer Werbekampagnen müssen die Hersteller auf den Produktpreis umlegen. Letztendlich zahlt der Kunde dafür, dass man ihn von den Vorzügen eines Produkts überzeugt. Dieses Argument führte Larry Augustin bei seiner Keynote auf dem Kongress Open Source Meets Business in Nürnberg an. Er legte in seinem Vortrag auch dar, dass sich die Marketingkosten proprietärer Produkte ungünstiger entwickeln als die Kosten freier Produkte. Im Idealfall vermarktet sich ein beliebtes Open-Source-Produkt von selbst (obwohl die Realität sicherlich weniger günstig aussieht).

Pikanterweise liegt ein Grund für den Anstieg der Marketingkosten sicher auch in der einfachen Verfügbarkeit vieler gleichwertiger Open-Source-Alternativen. So unterstützt OSS ihren eigenen Aufstieg.

## Eine Community entsteht nicht automatisch

Synergien sind ein weiteres, häufig genanntes Argument für ein „Going Open Source“. Demnach können Unternehmen von der Arbeitskraft der Open-Source-Community profitieren, die etwa Verbesserungen zu einer Software beiträgt.

Es ist sicherlich nicht zu bestreiten, dass beispielsweise Fehlerberichte einer großen Community zur Qualität einer Software beitragen. Besonders wichtig ist auch der Aspekt der kundengerechten Entwicklung. Sie kann sich bei einer Open-Source-Software zum Automatismus entwickeln – die Produktentwicklung erfolgt nicht mehr für den Markt, sondern mit ihm.

Aber gerade in der gemeinsamen Entwicklung mit einer externen Community lauert der Teufel im Detail. Zunächst einmal ist die Software nur eine Komponente des Open-Source-Business-Modells. Bei reiner OSS wird das Geld mit anderen Geschäftsbereichen (insbesondere den Dienstleistungen) verdient. Änderungen an der Basissoftware wirken sich deshalb oft nicht unmittelbar auf diese Geschäftsbereiche aus.

Sind Lizenzumsätze etwa im Rahmen des Dual Licensing eingeplant, muss man die Rechte berücksichtigen, die externe Programmierer durch ihre Softwarebeiträge möglicherweise an Teilen des Softwareprodukts erhalten. Im Extremfall ist man nicht mehr Herr über das vormals eigene Erzeugnis. Viele Unternehmen akzeptieren externe Anteile deshalb nur, wenn ihnen die Autoren alle notwendigen Rechte einräumen, um unabhängig agieren zu können. Sinnvolle externe Beiträge wird man aber nur mit einer entsprechend großen und loyalen Nutzer- und Entwicklergemeinde erhalten. Schränkt man deren Rechte ein, so wirkt man dem Aufbau dieser Gruppe direkt entgegen. Es gibt viele Gründe für einen Entwickler, an Open-Source-Produkten mitzuarbeiten. Anderen zu Reichtum zu verhelfen gehört aber sicherlich nicht dazu. Ohne die Nutzergemeinde ist eine Open-Source-Strategie jedoch sinnlos.

Bei sehr umfangreichen Anwendungen ist es wahrscheinlich, dass der Hersteller zunächst eher von Bugreports als von Programmierbeiträgen profitiert. Ohne passende Dokumentation für alle Bereiche der Software dürfte es schwierig bis unmöglich sein, sich in ein Produkt mit im Extremfall Millionen von Zeilen Code einzuarbeiten. So bleibt der Community nur der Hinweis, was alles nicht funktioniert, nicht aber warum.

Nebenbei bemerkt sollte man der Community mit der Entscheidung für das „Going Open Source“ das Leben so einfach wie möglich machen. Hier helfen neben der genannten Dokumentation auch Diskussionsforen, Bugtracker und Veranstaltungen für Entwickler. Denn die Community ist die wichtigste Komponente einer Open-Source-Strategie.

## Fazit

Zum Schluss sei darauf hingewiesen, dass – nach Einschätzung des Autors – die Open-Source-Community von kommerziellen Aktivitäten fast ausschließlich profitiert. Jedem steht es frei, eine OSS (im Sinne der Definition der Open Source Initiative) nach eigenen Vorstellungen weiterzuentwickeln, wenn die Firma hinter einem Produkt den Kurs wechselt. Im Regelfall dürfte dies aber nicht passieren, und Nutzer erhalten die Möglichkeit, kostenlos von Millioneninvestitionen in ein Produkt zu profitieren. Und zu Beiträgen ist niemand gezwungen. Das Risiko des „Going Open Source“ liegt damit fast ausschließlich bei den Firmen.

Auch der Aspekt „Job-Maschine“ ist hier zu nennen. So zeigt eine im April veröffentlichte Untersuchung der Linux-Foundation, dass zwischen den Versionen 2.6.11 und 2.6.24 fast drei Viertel aller Veränderungen am Linux-Kernel von Firmenmitarbeitern stammten [c, d].

Wichtig ist aus Community-Sicht, dass jegliche Aktivitäten die Open-Source-Grundwerte nicht verwässern. Kernkomponenten müssen frei (im Sinne von „Free Beer“ und „Free Speech“) sein. Und Enthusiasmus wie Kultur freier Software darf man sich von den Herren in den grauen Anzügen nicht nehmen lassen. Dann kann sich das Business-Modell „Open Source“ zum Selbstläufer entwickeln, von dem alle profitieren. (avr)

DR. RÜDIGER BERLICH

ist Diplom-Physiker am Karlsruhe Institute of Technology. An der Steinbeis Hochschule Berlin bildet er sich zum Master of Business Administration mit Schwerpunkt „Open Source Business Modelle“ fort.

### Onlinequellen

| | | |
|---|---|---|
| [a] | IDC-Zahlen | www.idc.com/getdoc.jsp?containerId=prUS20711507 |
| [b] | Red-Hat-Geschäftsberichte | investors.redhat.com/phoenix.zhtml?c=67156&p=irol-reportsannual |
| [c] | Open Source Jahrbuch 2008 | www.opensourcejahrbuch.de |
| [d] | Analyse der Kernel-Quellen | www.linux-foundation.org/publications/linuxkerneldevelopment.php |

### Literatur

[1] Glyn Moody, Rebel Code; The Penguin Press, London 2001; ISBN 0-713-99520-3

[2] Philip Kotler et. al.; Grundlagen des Marketings; Pearson Studium, 4. aktualisierte Auflage 2005; ISBN-10: 3-8273-7176-7;






Kennzahlen und Messbarkeit der IT-Sicherheit

# Schutzfaktor

**Stefan Strobel**

Die Effektivität von Maßnahmen, die viel Geld kosten, möchten Controlling und Geschäftsführung möglichst durch entsprechende Kennzahlen belegt wissen – das gilt auch für IT-Sicherheit. Doch gerade abstrakte Größen lassen sich nur schwer in Zahlen fassen.




Der Begriff Kennzahl existiert nicht erst seit gestern in der IT-Branche. In größeren Unternehmen ist es seit Langem gängige Praxis, die Abläufe als Prozesse zu sehen und deren Effektivität mit Kennzahlensystemen zu überwachen und zu steuern. Wer sich im IT-Betrieb mit ITIL (IT Infrastructure Library) beschäftigt, sieht sich dort immer wieder mit der Forderung nach Kennzahlen beziehungsweise „Key Performance Indikatoren“ (KPIs) konfrontiert. Und wer sich als Controller mit Cobit (Control Objectives for Information and Related Technology) auseinandersetzt, findet auch in diesem Standard viele Verweise und Beispiele von Kennzahlen.

So ist es nicht verwunderlich, dass gerade Controller und Vertreter aus der Chefetage oft den Wunsch nach Kennzahlen und Effektivitätsmessungen an die IT-Sicherheitsverantwortlichen herantragen. Aber auch Sicherheitsmanager selbst sind in der Regel nicht abgeneigt, die eigene Arbeit und die kontinuierliche Verbesserung der Sicherheit in Form von Zahlen darstellen zu können – zumal der vielbeachtete Standard ISO 27001 hier entsprechende Forderungen formuliert.

Trotz all der nachvollziehbaren Motive, sich mit Kennzahlen für IT-Sicherheit zu beschäftigen, findet man kaum Firmen, die schon länger ein Kennzahlensystem für diesen Bereich etabliert haben und damit wirklich glücklich sind. Die meisten geben zu, dass es ihren Messwerten an Aussagekraft mangelt. Offenbar lassen sich viele Hoffnungen und Wünsche an Kennzahlen im Bereich der IT-Sicherheit nicht so einfach oder gar nicht realisieren, und das hat viele Gründe.

Schon Diskussionen über Kennzahlen in der IT-Sicherheit gestalten sich in der Regel schwierig, da die Diskussionsteilnehmer meist ein unterschiedliches Verständnis von Kennzahlen haben. Während sich Chefs gelegentlich eine Art Fieberthermometer oder Ampel für die Sicherheit des Unternehmens wünschen, auf der sie jeden Morgen aktuell sehen können, ob alles im grünen Bereich ist, versuchen die Verantwortlichen für einzelne Bereiche oder Systeme der IT-Sicherheit manchmal, den Erfolg der eigenen Arbeit in Zahlen zu fassen, um sie ihren Chefs zu präsentieren.

## Begriffswirrwarr allerorten

Dabei führen sie meist Fakten wie die Anzahl der am Gateway blockierten Viren oder Spam-E-Mails an, die durchaus die Existenz des Virenscanners und Anti-Spam-Systems rechtfertigen, aber aus Sicht eines Controllers nicht als echte Kennzahlen gelten (Abb. 1). Aus seiner Sicht sind Kennzahlensysteme ein wichtiges Werkzeug zur Steuerung der Prozesse im Unternehmen. Dazu werden die Kennzahlen in einem Regelkreislauf gegen Sollwerte verglichen und aus den Abweichungen kann man Maßnahmen ableiten, die auf das Objekt, also die Prozesse im Unternehmen, einwirken.

Es wäre falsch, nur einer der drei beispielhaft genannten Parteien Recht zu geben und zu behaupten, dass die anderen Interpretationen von Kennzahlen falsch wären. In der Praxis gibt es überdies mehr als die drei genannten Positionen, und die erste Herausforderung in Diskussionen über Kennzahlen in der IT-Sicherheit ist es, sich auf eine gemeinsame Ebene zu einigen, damit man nicht aneinander vorbeiredet.

Aber nicht nur der Begriff der Kennzahl selbst kann zu Schwierigkeiten führen. Schon der grundlegende Begriff der Sicherheit kann in diesem Zusammenhang Konflikte erzeugen. Wenn man die Sicherheit messen möchte, sollte man sich zunächst darüber einig sein, was man damit eigentlich meint. Und so trivial diese Fra-

ge klingen mag, in der Praxis ist sie alles andere als einfach. Die bestimmt allen bekannte Phrase „Sicherheit ist ein Prozess“ ist zwar schwer zu kritisieren, aber wer sie anführt, muss sich die Frage gefallen lassen, ob ein Unternehmen, das seine IT-Sicherheit in vielen Prozessen organisiert und sich dabei sogar am Standard ISO 27001 orientiert, dann zwangsläufig sicher ist.

Während eine Interpretation von Sicherheit im Kontext von Kennzahlen die Prozesse des Sicherheitsmanagements im Vordergrund sieht, kann man alternativ Sicherheit als ein akzeptables Niveau des Risikos betrachten. Im ersten Fall würden sich die Kennzahlen primär auf die Prozesse und deren Effektivität oder Einhaltung beziehen, während im zweiten Fall Ergebnisse aus Risikoanalysen und Bewertungen sowie Sicherheitsüberprüfungen und Audits interessant sind.



**Verschiedene Welten: Was für den Sicherheitsverantwortlichen messbare Größen und somit „Kennzahlen“ sind (links), hat mit den Kategorien des Controllers (rechts) herzlich wenig zu tun – und ist deswegen für ihn wenig brauchbar (Abb. 1).**

## Keine Kennzahl ohne Vergleichs

Wer es mit dem Begriff Kennzahl ganz genau nehmen möchte, findet in der Literatur einige Quellen, die den Rahmen enger stecken, als er bisher beschrieben wurde und gelegentlich umgangssprachlich verwendet wird. So sind Kennzahlensysteme im engeren Sinn tatsächlich Werkzeuge zur Steuerung von Prozessen im Unternehmen, und sie kommen vor allem aus der Welt der Controller. Wichtige Anforderungen bei der Entwicklung von Kennzahlen sind deshalb, dass man mit ihnen tatsächlich einen Prozess steuern kann. Dazu gehört zwingend, dass es für jede Kennzahl auch einen Sollwert gibt, mit dem man sie vergleichen kann, und dass man aus den gemessenen Werten Aktivitäten zur Verbesserung der Prozesse ableiten kann.

Die verschiedenen Guides der offiziellen Stellen sowie Standards zum Thema Kennzahlen, Messungen beziehungsweise Metriken in der IT-Sicherheit sehen dies ähnlich. Egal ob man den NIST 800-55, BIP0074 oder den kommenden ISO-Standard 27004 betrachtet, in allen Dokumenten geht es um Messungen der Effektivität von Sicherheitsmaßnahmen, um daraus eine kontinuierliche Kontrolle und Verbesserung der Maßnahmen abzuleiten, und in allen stehen die Prozesse und Policies eher im Vordergrund als einzelne technische Details.

Schon ISO 27001 sieht diese Effektivitäts-Messungen explizit vor. Konkret fordert der Standard, dass das Management definiert, wie die Effektivität der ausgewählten Sicherheitsmaßnahmen später zu messen ist. Und er fordert explizit, dass mit den Messungen reproduzierbare und vergleichbare Ergebnisse erzielt werden sollen.

Diese Forderungen stehen jedoch im klaren Gegensatz zu den heute verbreiteten Messungen in der IT-Sicherheit. Nach einer Umfrage des CSO-Magazins sind die häufigsten Metriken in diesem Bereich die Anzahl der in Dateien oder Mails gefundenen Viren, die Anzahl ungültiger Passworteingaben, die Anzahl erkannter Angriffsversuche sowie die Anzahl blockierter Spam-Mails im Monat. Alle diese Zahlen lassen sich relativ einfach aus den Reports oder Logs vorhandener Systeme entnehmen. Sie eignen sich jedoch kaum dazu, die Effektivität einer Maßnahme zu messen und aus Abweichungen vom Sollwert korrigierende Maßnahmen abzuleiten.

## Eine Zahl – viele Ursachen

Wenn beispielsweise ein Mail-Virenscanner in den vergangenen Monaten durchschnittlich 100 Viren pro Tag herausgefiltert hat und diese Zahl auf 300 Viren pro Tag ansteigt, kann man nicht einmal sagen, ob diese Veränderung gut oder schlecht ist. Die Steigerung könnte daran liegen, dass der Virenscanner nach einem Update eine deutlich bessere Erkennungsrate hat oder dass auf einmal deutlich mehr verseuchte Mails im Internet kursieren. Ein Sollwert lässt sich hier nicht finden. Im negativen Sinne lässt sich hier sehr treffend Albert Einstein zitieren, der einmal gesagt hat: „Nicht alles, was zählt, kann gezählt werden, und nicht alles, was gezählt werden kann, zählt.“

Ähnliches gilt für Messungen zur Effektivität eines Anti-Spam-Systems. Die am einfachsten zu erfassenden Zahlen sind die Anzahl der transportierten sowie der blockierten Spam-Mails. Eine korrekte Aussage zur Effektivität des Spam-Filters müsste jedoch auch die Anzahl der fälschlicherweise durchgelassenen Spam-E-Mails sowie die Zahl der fälschlicherweise blockierten berücksichtigen. Den meisten Unternehmen wird es dabei sicher wichtiger sein, dass möglichst wenige wichtige Mails fälschlicherweise blockiert werden, dafür nehmen sie eine gewisse Anzahl an durchgelassenen Spam-Mails in Kauf.

Die kontinuierliche Beschaffung dieser Basisdaten ist jedoch nicht trivial. Aber auch wenn die hier aufgelisteten Zahlen nicht als Kennzahlen im engeren Sinne durchgehen, sollte man sie nicht zu schlecht reden. Immerhin können sie die prinzipielle Funktion der jeweiligen Systeme zeigen, und das Management kann an den jeweiligen Statistiken sehen, dass die Investitionen, beispielsweise in einen Mail-Virenscanner, einen Effekt hatten.

Auf der Suche nach Beispielen, die auch im engeren

**iX-TRACT**

- Zur Überprüfung der Effektivität von Maßnahmen und Wirtschaftlichkeit von Investitionen bedarf es in aller Regel belastbarer Kennzahlen – die aber bei abstrakten, kaum messbaren Größen wie „Sicherheit“ nur schwer zu erhalten sind.
- Die bisherigen Ansätze zur Messbarkeit von IT-Sicherheit in verschiedenen Standards sind relativ oberflächlich und untechnisch – erfüllen aber gelegentlich dennoch ihren Zweck.
- Da das Thema Kennzahlen für die IT-Sicherheit noch in den Kinderschuhen steckt, kann man hier durchaus kreativ sein und ungewöhnliche Zahlen und Größen – beispielsweise das Schwachstellenmanagement – erfolgreich zur Beurteilung und Verbesserung von Prozessen heranziehen.

Sinne der Begriffsdefinition als gute Kennzahlen durchgehen, ist man geneigt, nochmals einen Blick in die genannten Standards zu werfen. In dem vom britischen BSI herausgegebenen Guide BIP 0074 mit dem Titel „Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001“ finden sich Beispiele wie „Completeness of Implementation“ für verschiedene Bereiche. Dabei könnte beispielsweise der Prozentsatz der tatsächlich eingerichteten Firewalls bezogen auf die Liste der geplanten beziehungsweise erforderlichen Firewall-Systeme als Kennzahl dienen.

## Aus Standards abgeleitet

Ein anderes Beispiel aus BIP 0074 wäre „Completeness of Backup“ oder „Testing of Backup“, ebenfalls als Prozentsatz der Server, für die regelmäßig ein Backup erstellt wird, beziehungsweise der Prozentsatz der Backups, die jemand regelmäßig daraufhin prüft, dass sie im Bedarfsfall auch zurückgespielt werden können.

Diese Beispiele sind nachvollziehbar, jedoch nicht überraschend. Ähnlich sehen diejenigen aus dem ISO-27004-Entwurf aus. Die Autoren nehmen die „Controls“ beziehungsweise „Control Objectives“ aus dem 27001-Standard als Leitfaden und nennen dafür Beispiele zur Messung der Effektivität. Die Weiterbildungsmaßnahmen für das IT-Sicherheits-Personal ließen sich demzufolge durch eine Auswertung der Mitarbeiterdatenbank anhand der Anzahl der tatsächlich besuchten Schulungen im Verhältnis zu den geplanten ermitteln.

Wer sich an dieser Stelle technischere Beispiele erhofft hat, ist nun sicher enttäuscht. Die in den Standards genannten bleiben auf einem eher trivialen Niveau, und der Begriff Sicherheit wird primär über seine Prozesse definiert. Positiv überraschen die angeführten Modelle selten.

Ein Highlight für Liebhaber technischer Lösungen ist dabei vermutlich ein Beispiel zur Messung der Effektivität von Passwort-Regeln. Der 27004-Entwurf schlägt vor, regelmäßig mit einem Passwort-Cracker zu prüfen, welchen Anteil der Passwörter dieser innerhalb von 4 Stunden knacken kann. Diese Messung kann man sicherlich kontrovers diskutieren, denn das Ermitteln von Benutzerpasswörtern an sich kann in einem Unternehmen mit kritischem Betriebsrat durchaus problematisch sein. Dennoch führen einige Firmen die „Messungen“ in dieser oder einer ähnlichen Form durch.

## Audits als Basis für Messbarkeit

Neben der eigenen Ermittlung von Kennzahlen findet man immer wieder auch Beispiele von Beratungsunternehmen, die für sich in Anspruch nehmen, nach einer eigenen Methode oder auf Basis der etablierten Standards die Sicherheit ihrer Kunden so zu prüfen, dass dabei Kennzahlen herauskommen, die man auch zum Vergleich zweier Organisationen heranziehen kann. Meist führen diese Beratungsunternehmen Interviews durch, um die Umsetzung von Maßnahmen aus einem vorgegebenen Katalog abzufragen. Faktisch handelt es sich also um eine nichttechnische Variante des klassischen externen Audits.

Generell ist die Bewertung der eigenen Sicherheit durch externe Prüfer, egal ob man dabei von Audits oder sogenannten Penetrationstests (Einbruchstests) spricht, auf technischer oder auf organisatorischer Ebene eine Herangehensweise, die etabliert ist und auch in Zukunft nicht an Bedeutung verlieren wird. Der ISO-Standard 27001 verweist darauf, dass die Ergebnisse von Audits und Penetrationstests in den kontinuierlichen Weiterentwicklungs-Zyklus einbezogen werden sollten.

Wenn man jedoch die Ergebnisse solcher Prüfungen auf harte Zahlen abbilden möchte, muss man berücksichtigen, dass es sich in der Praxis kaum vermeiden lässt, dass die Ergebnisse auch von den Prüfern abhängen und dass darunter die Reproduzierbarkeit und Vergleichbarkeit etwas leidet. Inwieweit es sinnvoll ist, solche Zahlen überdies noch zum Vergleich zwischen unterschiedlichen Organisationen heranzuziehen, ist eine ganz andere Diskussion, denn jedes Unternehmen hat seine eigenen zu schützenden Werte, Sicherheitsziele und Policies.

Der eine oder die andere wird sich nun vermutlich fragen, ob es denn keine Produkte zu kaufen gibt, die als Ergebnis verwertbare Kennzahlen und eine Bewertung der Sicherheit im Unternehmen produzieren. Und tatsächlich gibt es eine Klasse von Produkten beziehungsweise Hersteller, deren Marketing und Vertriebsleute genau das versprechen. Die Rede ist von Security-Information-and-Event-Management-Systemen (SIEM), also Produkten, die an zentraler Stelle Logs und Events sammeln, normalisieren, korrelieren und archivieren oder auswerten. In den Broschüren und Vertriebsvorträgen dieser Anbieter findet man nicht selten das Versprechen, dass sowohl Kennzahlen als auch ein Überblick und die Bewertung der Sicherheit Anschaffungsgründe für solche Systeme seien.

Bei genauerer Betrachtung erkennt man jedoch schnell, dass hinter diesen Versprechungen wenig Substanz steckt. Selbstverständlich ist eine zentrale Logfile-Auswertung aus Sicherheitserwägungen durchaus erstrebenswert und sinnvoll. Auch die Beschaffung von Basisdaten für Kennzahlen, die aus Logs kommen, wird mit einem solchen System einfacher, da alle Logs an zentraler Stelle erreichbar sind. Nur kann ein SIEM-System auch keine Kennzahlen herzaubern, die ohne ein solches System nicht schon ermittelbar gewesen wären.

## Schwachstellen-analyse einbeziehen

Ein anderer Ansatz zur teilweise automatischen Ermittlung von Kennzahlen basiert auf dem Verwundbarkeits- oder Schwachstellen-Management. Da Schwachstellen ein wesentlicher Einflussfaktor des technischen Sicherheitsrisikos sind, ist es sinnvoll, die Ergebnisse von Verwundbarkeits-Scannern als Basisdaten zur Ermittlung von Kennzahlen heranzuziehen. Vorraussetzung dafür ist aber, dass ein Prozess zum regelmäßigen, vergleichbaren und konsistenten Scannen der internen oder auch externen Systeme etabliert ist.

Hilfreich dafür sind die bekannten Enterprise-Scanning-Produkte, die nach definierten Policies mit optional verteilten Scan-Appliances automatisch nächtliche oder wö-

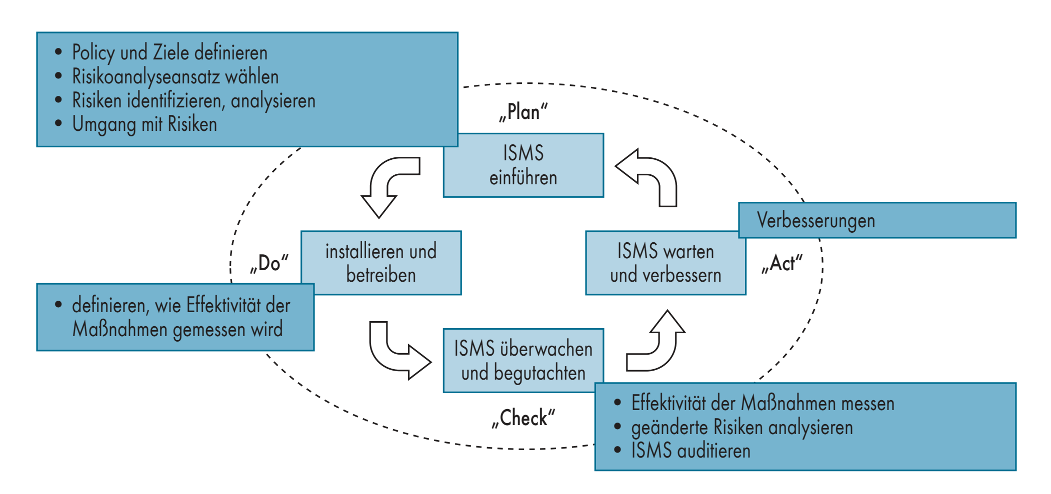
**Onlinequellen**

| | |
|---|---|
| ISO/IEC 27001: Information security management systems – Requirements | www.iso.org |
| ISO/IEC 27004: Information security management measurements | www.iso.org |
| BIP 0074 | www.bsi-global.com |
| NIST 800-55: Security Metrics Guide for Information Technology Systems | csrc.nist.gov/publications/nistpubs |
| CobiT 4.0 / 4.1 | www.isaca.org |

chentliche Scans durchführen und die Ergebnisse in einer zentralen Datenbank bereitstellen. Ein Beispiel für solche Kennzahlen wäre die durchschnittliche Anzahl kritischer Schwachstellen auf den als wichtig klassifizierten Serversystemen.

Die nächste Stufe dieses Ansatzes ist, dass man nicht nur die Verwundbarkeiten betrachtet, sondern auch die daraus resultierenden möglichen Angriffsvektoren auf wichtige Applikationen. Mehrere Hersteller bieten Produkte an, die die Ergebnisse von Enterprise-Scannern mit der Konfiguration der Router und Firewalls im Unternehmen zusammenbringen und daraus die tatsächlich durchführbaren Angriffsketten und deren Ausnutzungswahrscheinlichkeit errechnen. Für die wichtigsten Grundwerte der Organisation beziehungsweise für die entsprechenden Applikationen können dann Prioritäten oder sogar Werte hinterlegt werden, damit nicht nur Bedrohungsvektoren, sondern auch die benötigten Schadenshöhen in die Risikorechnung einfließen.

Mit solchen Mechanismen sind fast vollständig automatisierte Aussagen über das technische Sicherheitsrisiko möglich. Wenn man über diesen Weg Kennzahlen ermittelt, sollte man sich jedoch bewusst sein, dass auch diese Kennzahlen nur einen Teilbereich abdecken. Weiche Faktoren, die Mitarbeiter, deren Sensibilisierung und ähnliche Einflussfaktoren, die möglicherweise sogar den größten Teil des Risikos ausmachen, sind in solchen Berechnungen nicht enthalten.




**Das „Plan-Do-Check-Act-Modell" des ISO 27001 sieht an mehreren Stellen Messungen der Effektivität von IT-Sicherheitsmaßnahmen vor. Orientieren kann man sich dabei an verschiedenen Standards, auch wenn sich deren Beispiele zurzeit noch im Anfangsstadium befinden (Abb. 2).**

## Fazit

Kennzahlen in der IT-Sicherheit sind kein einfaches Thema. Es gibt keine universellen Lösungen, die jeden befriedigen oder überzeugen. Unterm Strich muss zunächst jeder selbst entscheiden, was er mit den gesuchten Kennzahlen überhaupt erreichen will. Geht es primär um internes Marketing, um der Geschäftsleitung plausibel zu machen, dass IT-Sicherheit wichtig ist und dass die getätigten Investitionen sinnvoll waren, dann wird man gelegentlich auch Messungen präsentieren müssen, die keine Kennzahlen im engeren Sinne sind.

Geht es jedoch um die Kontrolle von Maßnahmen im Rahmen eines Information-Security-Management-Systems nach ISO 27001 (Abb. 2), sollte man durchaus nach Kennzahlen suchen, mit denen sich auch Prozesse steuern lassen, und sich dabei im ersten Schritt an den Beispielen aus BIP 0074 oder ISO 27004 orientieren – auch wenn diese sehr einfach gestrickt sind und wenig mit technischen Details zu tun haben. Kennzahlen auf der Grundlage von Verwundbarkeitsinformationen belegen, dass es noch mehr Möglichkeiten gibt, Kennzahlen zu definieren. Der Kreativität sind hier noch lange keine Grenzen gesetzt – zumal das Thema für die IT-Sicherheit gerade erst in den Kinderschuhen steckt. (ur)


STEFAN STROBEL

ist Geschäftsführer und Mitbegründer des Heilbronner Security-Beratungsunternehmens Cirosec.


### Literatur


[1] BIP 0074: Ted Humphreys, Angelika Plate, British Standard Institution; Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001 (www.bsi-global.com)

[2] Andrew Jaquith; Security Metrics, Addison-Wesley (www.securitymetrics.com)

[3] Martin Kütz, Kennzahlen in der IT, dpunkt-Verlag 2006








Modellgetriebene Softwareentwicklung für eingebettete Systeme mit Eclipse

# Grüne Welle

**Marc Habiger, Andreas Mülder**



Entwickler, die für eingebettete Systeme programmieren, müssen nicht nur die spezifischen Besonderheiten von Betriebssystemen und Hardware berücksichtigen, sondern unter anderem auch Aspekte wie Echtzeitverhalten und Zuverlässigkeit. Wie die modellgetriebene Entwicklung mit einer auf Eclipse basierenden Werkzeugkette hier helfen kann, zeigt das Beispiel einer Ampelsteuerung.

Längst haben die eingebetteten Systeme ihr Nischendasein verlassen und Einzug in den Alltag gehalten. Ohne es zu merken, interagieren viele Menschen ständig mit ihnen, beispielsweise mit Unterhaltungselektronik, Haushaltsgeräten oder im Pkw. Glaubt man aktuellen Studien ([1], [2]), wird sich dieser Trend noch beschleunigen und schon 2015 wird die meiste Software nicht mehr für konventionelle, sondern für embedded Systeme geschrieben. Vor diesem Hintergrund starteten 2006 drei Projektpartner das Forschungsprojekt „Modellgetriebene Softwareentwicklung für Embedded Systems“ [3], aus dem sich ein Praxisworkshop zur Einführung in die Kernkonzepte entwickelte. Auf einige Ergebnisse des Projekts geht dieser Artikel ein.

Die Softwareentwicklung in diesem Bereich steht vor heterogenen Herausforderungen. So unterscheiden sich die meisten eingebetteten Systeme hinsichtlich der zugrunde liegenden Plattform und der zur Verfügung stehenden Hardwareressourcen stark voneinander.

Nicht-funktionale Anforderungen wie das Echtzeitverhalten und die Zuverlässigkeit eines Systems spielen ebenfalls eine wesentliche Rolle bei der Entwicklung. Versagt beispielsweise das Steuergerät eines Satelliten, kann dies zu hohem wirtschaftlichen Schaden führen, im schlimmsten Fall bei lebenskritischen Systemen sogar Menschenleben gefährden. Auch die Testbarkeit eingebetteter Systeme kann sich als schwierig erweisen, wie am Beispiel des erwähnten Satelliten deutlich wird.

Die zunehmende Komplexität der Software ist ein weiterer Aspekt, den es zu berücksichtigen gilt – nicht ohne Grund initiierte der Bitkom 2007 den Arbeitskreis „Softwareintensive eingebettete Systeme“. Nicht nur bezüglich der heutigen Rechenleistung und Speicherkapazität vieler Embedded-Plattformen ist die klassische, manuelle Implementierung in rein imperativen Programmiersprachen oft nicht mehr angemessen. Auch die vielen unterschiedlichen Varianten, Vernetzung und die Verteilung von Softwarekomponenten auf unterschiedliche Hardware ist irgendwann nicht mehr direkt handhabbar, geschweige denn zu überblicken. Als Beispiel kann hier der AUTOSAR-Standard dienen, der dazu dient, die Softwarekomponenten der Automobilzulieferer zu beschreiben und mit dessen Hilfe das informationstechnische Gesamtsystem – also das Fahrzeug – konfiguriert wird.

## Domänenspezifische Werkzeuge

Ein Ansatz, diese Herausforderungen zu bewältigen, ist die modellgetriebene Softwareentwicklung. Neben der aus Validierungen auf höherer Abstraktionsebene und Codegenerierung resultierenden höheren Qualität und Produktivität ist es von Vorteil, dass sich die Komplexität der Artefakte und die plattformspezifischen Aspekte weitgehend verbergen lassen. Entwickler können sich so besser auf die eigentliche Aufgabe, das Implementieren von Programmlogik, konzentrieren, während sich schematische Routineaufgaben weitgehend über Codegeneratoren erledigen lassen. Auch die Wiederverwendung einzelner Komponenten ist tendenziell besser. Im Gegensatz zu CASE-Tools unterstützen gute MDSD-Frameworks (Model-Driven Software Development) viele unterschiedliche Modelle, man ist also nicht an eine Modellierungsart, beispielsweise die UML (Unified Modeling Language), gebunden.

Um den größtmöglichen Vorteil aus der modellgetrie-

benen Entwicklung eingebetteter Systeme zu erzielen, setzt man am besten eine integrierte Entwicklungsumgebung (IDE) ein, die Werkzeuge für die jeweilige Domäne bereitstellt und den Entwickler in allen Aspekten des Softwareentwicklungsprozesses unterstützt. Dabei reicht das Werkzeugspektrum von textuellen und grafischen Editoren zum Modellieren und Validieren von Software über Simulatoren bis hin zu Codegeneratoren, automatisierten Tests und Deployment.

Die hier vorgestellte Werkzeugkette basiert zum größten Teil auf Eclipse, einer hervorragenden Plattform für Werkzeugintegration. Es gibt zahlreiche Projekte, die das Entwickeln eigener Tools unterstützen, etwa das Eclipse Modeling Project. Abbildung 1 zeigt die verwendeten Techniken (blau) und die Werkzeuge (gelb), die darauf aufsetzen.

Das Eclipse Modeling Framework (EMF) bietet Unterstützung bei der Erzeugung und Bearbeitung von Modellen. Darauf setzt openArchitectureWare auf, das mit der Template-Sprache Xpand das Entwickeln von Codegeneratoren und mit xText die Erzeugung textueller Editoren ermöglicht. Das Graphical Editing Framework (GEF) und das Graphical Modeling Framework (GMF) erleichtern die Entwicklung grafischer Editoren und setzen ebenfalls auf dem EMF auf.

Zum Bearbeiten des C-Codes, Kompilieren, Linken und Debugging dienen die C Development Tools (CDT), die Eclipse um C/C++-spezifische IDE-Funktionen erweitern.

## Fußgängerampel als Praxisbeispiel

Ein gängiges Fallbeispiel – die Steuerung einer Fußgängerampel, die auf einem 8-Bit-Mikrocontroller läuft und auf einem Display visualisiert wird – soll die modellgetriebene Entwicklung eines eingebetteten Systems veranschaulichen. Ein alternatives Generierungsziel erlaubt den Anschluss einer externen Peripherie mit realen Ampelleuchten und demonstriert damit einen der wesentlichen Vorteile dieses Vorgehens: die Abstraktion zwischen Modell und Zielplattform.

Zum Modellieren von Verhalten dienen Zustandsautomaten, wie sie aus der UML bekannt sind. Hierzu wird ein eigener grafischer Editor eingesetzt, der – wie weiter unten noch zu sehen sein wird – um eine aktive Kommunikationsschnittstelle für die interaktive Simulation erweitert wurde. Abbildung 2 zeigt den Zustandsautomat für eine einfache Ampel.

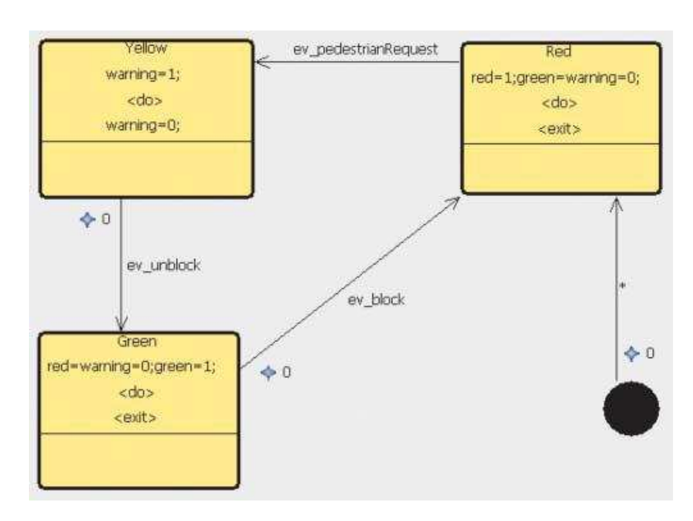
Das Modell besteht aus den drei Zuständen *Red*, *Yellow* und *Green* sowie einem Startzustand. Die Zustandsübergänge (Transitionen) lassen sich durch Events auslösen. So führt das Ereignis *ev_pedestrianRequest* beispielsweise dazu, dass die Anwendung

**iX-TRACT**

- Die modellgetriebene Softwareentwicklung erleichtert auch die Anwendungsprogrammierung für eingebettete Systeme.
- Durch das höhere Abstraktionsniveau lassen sich für diverse Bereiche unterschiedliche Anforderungen formulieren, die ein Generator in plattformspezifische Programme übersetzen kann.
- Hilfe während des Entwicklungsprozesses kann die Eclipse-IDE leisten, die sich bei Bedarf um passende Werkzeuge ergänzen lässt.

textueller Editor / Codegenerator | grafischer Editor | CDT
openArchitectureWare | GEF / GMF
EMF
Eclipse

**Eine auf Eclipse basierende Werkzeugkette unterstützt die modellgetriebene Entwicklung (Abb. 1).**




**Der Zustandsautomat für eine einfache Ampel: Variablen und Events lassen sich den Ein- und Ausgängen der Zielplattform zuordnen (Abb. 2).**

vom Zustand *Red* zu *Yellow* wechselt. Beim Eintritt in einen Zustand führt das Programm die *Entry*-Action aus, in Fall des Zustands *Yellow* setzt dies die Variable *warning=1*. Diese Variablen und Events lassen sich nun den Ein- und Ausgängen der Zielplattform zuordnen (siehe unten).

Der nächste Schritt soll das Beispiel zu einem vollwertigen Fußgängerüberweg ausbauen. Eine Alternative wäre, den Zustandsautomat um die fehlenden Funktionen zu ergänzen, was allerdings schnell zu einem großen, unübersichtlichen und schlecht wartbaren Zustandsautomaten führen würde. Daher bietet die Werkzeugkette die Möglichkeit, mehrere Zustandsautomaten miteinander zu verbinden, sodass Events untereinander austauschbar sind. Hierbei hilft ein textueller Editor aus eigener Entwicklung, der über eine spezielle, domänenspezifische Sprache (DSL) das Verbinden von Blöcken ermöglicht und vom zugrunde liegenden Programmcode abstrahiert.

Listing 1 zeigt ein vereinfachtes Beispiel des textuellen Modells mit zwei Zustandsautomaten: einem Controller und der Fußgängerampel. Der Controller übernimmt die Koordination der Ampel (in Abbildung 2 ist er nicht abgebildet).

Das hier abgebildete Modell besteht aus zwei Abschnitten. Im ersten lassen sich Blöcke definieren. Nach dem Schlüsselwort *block* steht ein eindeutiger Name gefolgt vom Blocktyp, der in diesem Beispiel *StateChart* ist. Hierauf folgen eine Reihe frei definierbarer Ein- und Ausgänge, denen man einen frei wählbaren Namen geben kann.

Abhängig vom Blocktyp lassen sich die Instanzparameter festlegen. Da die Beispielblöcke vom Typ *StateChart* sind, gibt es nur einen blockspezifischen Parameter: *path*. Er gibt den eigentlichen Zustandsautomaten an, der mit-

**Listing 1**

```
block Controller isa StateChart
{
    in pedestrianRequest
    out blockPedestrianTrafficLight;
    out unblockPedestrianTrafficLight;
    param path="crossing.statemachine";
    param blockname="Controller";
}
block Pedes isa StateChart
{
     in unblock;
      in block;
       out red;
      out green;
       param blockname="Pedes";
      param path="Pedes.statemachine";
}
connect Controller.blockPedestrianTrafficLight with Pedes.block;
connect Controller.unblockPedestrianTrafficLight with Pedes.unblock;
```

**Die zwei Zustandsautomaten *Controller* und *Pedes* lassen sich miteinander verbinden.**

**Listing 2**

```
interface {
   // outputs
   out Pedes.red type bit ;
   out Pedes.green type bit ;
}
```

**Das Interface beschreibt die Außensicht eines Modells. Für die Generierung des auf eine konkrete Hardware passenden Codes sorgt ein Mapping.**

**Listing 3**

```
mapping EvaluationBoardHardware
   template "traffic_lights" start Main
{
   // used templates
   templates {
        writePort
   }

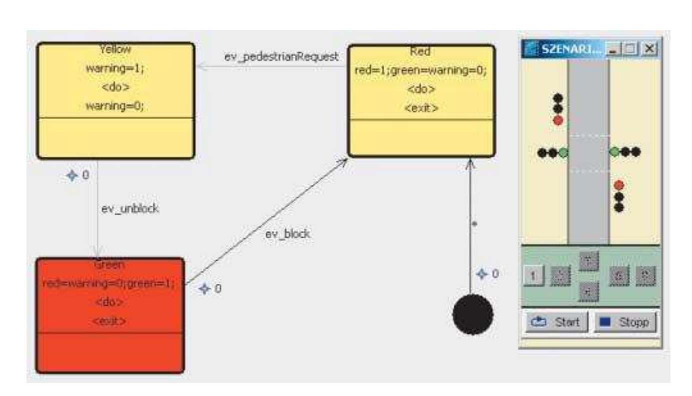
output Pedes.red => {using writePort:
                 port="PORTA" bit="1"}
output Pedes.green => {using writePort:
                 port="PORTA" bit="4"}
}
mapping AnotherHardware
   template "demo_template" start Main
{
   ....

}
```

hilfe des grafischen Editors modelliert wurde.

Im zweiten Teil der Grammatik können die Ein- und Ausgänge der Blöcke miteinander verbunden werden. Dies geschieht nach der Form *connect <Blockname>.<Ausgang> „with“ <Blockname>.<Eingang>*. Eine Besonderheit stellt die Verbindung der Ausgänge dar, die direkt mit der Hardware interagieren, wie im vorliegenden Fall die Ausgänge *Pedes.red* und *Pedes.green*. Mehr dazu unten.

Ein Block ist in diesem Kontext eine zeitdiskrete, parametrierbare Komponente, die Ein- und Ausgänge mit weiteren Blöcken verbinden können. Diese Art der komponentenbasierten Modellierung bietet eine Reihe von Möglichkeiten. Komplexes Verhalten lässt sich in einzelne Blöcke, die miteinander interagieren, zerlegen und bleibt so leicht verständlich und gut wartbar. Außerdem ist man nicht an Zustandsautomaten gebunden, sondern kann jede Art von Komponenten einbinden.




**Simulationskomponenten erlauben es, Modelle visuell zu testen (Abb. 3).**

## Mapping auf die richtige Hardware

Die hier vorgestellte Werkzeugkette unterstützt bereits viele aus der Steuerungs- und Regelungstechnik bekannte Blöcke. Durch das Komponentenkonzept kann ein Entwickler die Werkzeugkette leicht erweitern. Beispielsweise wären Editoren mit einer regelbasierten Grammatik denkbar, die es erlauben, Verhalten textuell zu beschreiben.

Eine „Lücke“ besteht noch zwischen dem erzeugten Code aus den Modellen und der konkreten Hardware. Je nach Ausführungsumgebung gestaltet sich der Zugriff auf die Hardware völlig unterschiedlich. Dies kann von einer kompletten Hardwareabstraktion unter einem Betriebssystem bis hin zu C-Makros oder Inline-Assembler reichen. Diese Varianzen sind bei eingebetteten Systemen naturgemäß viel größer als bei Desktop-Systemen. Ob man sich für eine rein manuelle Implementierung oder einen generativen Ansatz entscheidet, hängt natürlich von der Zahl der möglichen Kombinationen beziehungsweise der Anzahl der Zielsysteme für ein Modell ab.

Der hier vorgestellte Ansatz besteht aus einer textuellen DSL zur Beschreibung des Modell-Interface und beliebiger Zuordnungen (Mapping) auf die Ausführungsumgebung sowie den dazugehörigen Code-Templates. Das Interface beschreibt die Außensicht des Modells, während einzelne Mapping-Abschnitte die jeweilige Brücke zum Zielsystem schlagen. Grundsätzlich wird hier nur ein Port des Modells mit einem Code-Template samt beliebigen Parametern assoziiert. Weitere Hinweise, etwa zur Gruppierung, können das Template bei der Codegenerierung beeinflussen. Der Editor bietet wie gewohnt weitreichende Unterstützung beim Editieren, und Checks sorgen unter anderem dafür, dass jedes Element des Interface in jedem Mapping zugeordnet wurde.

Der durch den Generatorlauf erzeugte C-Code ist direkt in den Build-Prozess integrierbar. Will man Code für eine andere Hardware generieren, genügt ein geänderter Parameter für den Mapping-Generator.

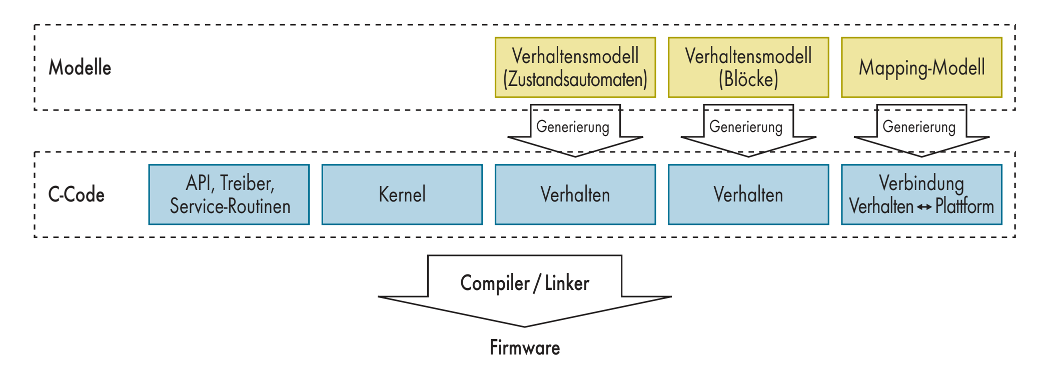
Ein essenzieller Aspekt bezüglich der Produktivitäts- und Qualitätssteigerung ist eine möglichst frühe Validierung auf Modellebene. Hierdurch lassen sich einerseits häufige Modellierungsfehler, die sich nicht automatisch aus der Struktur des Metamodells ergeben, frühzeitig erkennen und andererseits fachliche Bedingungen definieren. In der Werkzeugkette wird hierzu die Sprache Check, Bestandteil des MDSD-Frameworks openArchitectureWare, verwendet.

Durch die nahtlose Integration von Check in Eclipse wird dem Modellteil, das eine definierte Regel verletzt, automatisch ein sogenannter Problem Marker hinzugefügt, was sowohl in den textuellen als auch in den grafischen Editoren möglich ist. Ein weiterer Vorteil bei der Verwendung von Check liegt darin, dass die Entwicklungsumgebung eine Regelverletzung „live“ erkennt. Die oft langwierigen Code-Compile-Zyklen entfallen. Der folgende Code-Ausschnitt zeigt ein simples Beispiel für Validierungsregeln:

```
context State ERROR "A state must ⏎
                  have a name" :
  this.name != null && this. ⏎
              name.trim().length > 0;
```

Dem Schlüsselwort *context* folgt das Modellelement aus dem Metamodell, für das die Validierungsregel gelten soll.

Bei einer Regelverletzung kann entweder eine Warnung oder ein Fehler angezeigt werden, was die Schlüsselwörter *ERROR*, wie in diesem Beispiel, beziehungsweise *WARNING* festlegen. Dem Schlüsselwort folgt ein einfacher Zeichen-String mit der gewünschten Fehlermeldung. Nach dem Doppelpunkt steht der Validierungsausdruck. Liefert dieser *false* zurück, handelt es sich um eine Regelverletzung und der Problem Marker wird gesetzt.




**Der Generator erzeugt die Firmware aus verschiedenen Codequellen (Abb. 4).**

## Simulation hilft beim Debugging

Zur Simulation verwendet die Beispielwerkzeugkette eine kommerzielle Komponente namens BORIS (Blockorientiertes Simulationssystem), Teil des Programms WinFACT. Sie bietet die Möglichkeit, Simulationskomponenten auf einfache, grafische Weise zu erstellen und so die Modelle visuell zu testen. Hierzu sind die im Blockschaltdiagramm vorhandenen Zustandsautomaten mit dem grafischen Zustandseditor in Eclipse gekoppelt.

Dies ist besonders für das Debugging interessant, denn so kann beispielsweise leicht nachvollzogen werden, in welchem Zustand ein Fehler aufgetreten ist. Abbildung 3 zeigt die Visualisierungskomponente und einen damit verbunden Zustandsautomaten. Hier wäre in Zukunft ein einheitlicher Standard für Simulationsschnittstellen wünschenswert, um nicht für jede Anwendung eine komplett eigene Lösung entwickeln zu müssen.

Die Beispielanwendung erzeugt natürlich nicht die gesamte Firmware des Controllers aus dem Modell. Als Basis dient FreeRTOS [4], ein kompakter Open-Source-Echtzeitkernel mit grundlegenden IPC-Fähigkeiten. Darauf setzt eine dünne Treiberschicht auf, die mit der Hardware kommuniziert. Einige Grafik-API-Funktionen erlauben das komfortable Ansprechen eines Farbdisplays. Aus dem Modell wird schließlich der Code für das Verhalten erzeugt. Abbildung 4 gibt einen Überblick über die einzelnen Codequellen.

Der Build-Prozess des Generators bietet weitreichende Flexibilität, da man mit wenig Aufwand eigene Komponenten hinzufügen kann. Ein wesentlicher Teil der Generierung erfolgt in den XPand-Templates von openArchitectureWare. Anhand einer Referenzimplementierung lassen sich Schritt für Schritt mit dieser mächtigen Template-Sprache, die durch die Sprache Xtend unterstützt wird, eigene Codegeneratoren bauen.

Grundsätzlich kennt das Generat aus dem Modell keine Möglichkeit, seine Eingangsdaten zu beschaffen oder diese auszugeben. Da dies plattform- und API-spezifisch ist, muss hier noch eine Zuordnung der Ein- und Ausgabe vorgenommen werden, die aus dem erwähnten Mapping-Modell erzeugt wird, das die Modellschnittstelle den tatsächlichen Plattformfunktionen zuordnet.

Üblicherweise arbeiten Entwickler mit einer Reihe von Werkzeugen, die sie weiterverwenden wollen oder müssen. Gibt es für bestimmte Aufgaben oder Kommandozeilen-Tools noch keine Eclipse-Integration, ist die Erstellung von entsprechenden Plug-ins recht einfach. Das nahtlose Einbinden eines externen Programms in die IDE lässt sich oft mit wenig Aufwand erledigen. Im Beispiel wird das Tool zum Programmieren des Controllers und jenes zum Starten der Debugging-Software als Knopf in der Werkzeugleiste zur Verfügung gestellt.

Das Deployment erfolgt seriell über die RS232-Schnittstelle und einen Bootloader. Der Bootloader ist ein kleines Programm, das Firmwaredaten über anwenderspezifische Quellen einlesen und in den eigenen Programm-Flash schreiben kann.

## Fazit

Die modellgetriebene Softwareentwicklung kann helfen, die zunehmende Komplexität eingebetteter Systeme beherrschbar zu gestalten. Solange die Universal-IDE, die für jede Domäne die passenden Werkzeuge bereitstellt, noch nicht erfunden (und vielleicht auch nicht wünschenswert) ist, bietet sich Eclipse als Plattform für Werkzeugintegration an. Mit verhältnismäßig geringem Aufwand lassen sich individuelle Lösungen entwickeln und nahtlos in den bestehenden Softwareprozess integrieren, ohne dass Lizenzkosten anfallen.

Eine schrittweise Verbesserung der Werkzeugkette in einem fortlaufender Prozess erhöht die Akzeptanz bei den Softwareentwicklern. Denn diese müssen sich nicht von heute auf morgen an eine neue Entwicklungsumgebung gewöhnen. (ka)


MARC HABIGER

ist Hard- und Softwareingenieur bei der itemis AG. Neben der modellgetriebenen Softwareentwicklung befasst er sich mit embedded Hardware und hardwarenaher Programmierung.

ANDREAS MÜLDER

arbeitet als Softwarearchitekt bei der itemis AG. Seine Schwerpunkte liegen im Bereich modellgetriebene Softwareentwicklung und Werkzeugketten mit Eclipse.


### Literatur


[1] Roland Berger; Zukunft digitale Wirtschaft; Studie im Auftrag des Bitkom; www.bitkom.de/files/documents/Zukunft_digitale_Wirtschaft_BITKOM-Roland_Berger_Studie.pdf

[2] Kerstin Cuhls, Simone Kimpeler; Delphi-Report: Zukünftige Informations- und Kommunikationstechniken; Fazit Schriftenreihe Band 10

[3] Forschungsprojekt: Modellgetriebene Softwareentwicklung für Embedded Systems; www.mda4e.org

[4] The FreeRTOS.org Project www.freertos.org







Open Source ESBs: Mule und Service Mix

# Ansecksysteme

**Markus Demolsky, Alexander Schatten**



**Seit Anbeginn der elektronischen Datenverarbeitung diskutieren die Protagonisten darüber, wie sich die unterschiedlichen Anwendungen am besten unterhalten können. Den momentanen Stand der Technik markieren die Enterprise-Service-Busse, die auch kompetente Open-Source-Vertreter zu bieten haben.**

Softwaresysteme entstehen nur selten auf der grünen Wiese. In der Regel möchten Unternehmen ihre altgedienten Anwendungen weiter nutzen und darauf aufbauend neue erstellen. Der Wunsch: ein vollständig verdrahtetes Applikationsnetzwerk. Vor nicht allzu langer Zeit schloss man jedes zusätzliche System über einen speziell dafür entwickelten Adapter an. Leider ist die Wartung der zahllosen Konnektoren extrem aufwendig. In den letzten Jahren haben sich deshalb andere Integrationsstrategien herausgebildet, etwa die Nutzung gemeinsamer Dateien und Datenbanken, Methodenaufrufe über Remote Procedure Calls oder Webservices sowie Message Oriented Middleware (MOM).

ETL-Techniken (Extract, Transform, Load) wie File-Transfer oder Stapelverarbeitung sind nach wie vor die beliebteste Integrationsvariante. Nicht selten erzeugen solche Lösungen jedoch inkonsistente Daten auf den beteiligten Systemen. Tritt beispielsweise ein Fehler auf, muss der Job gegebenenfalls neu gestartet werden. Und abgebrochene Transaktionen führen gelegentlich zu Datenverlusten. Dass Batch-Jobs oft in der Nacht laufen, begrenzt ihre Laufzeit. In Umgebungen, die rund um die Uhr verfügbar sein müssen, sind die beschriebenen Techniken nicht praktikabel.

EAI-Broker (Enterprise Application Integration) haben sich Mitte der 90er-Jahre in der Industrie einen Namen gemacht. Sie erledigen das zentrale Routing zwischen den Applikationen und markieren einen Schritt auf dem Weg zu einer echten losen Kopplung der Anwendungskomponenten. Für die regionale Integration reichten EAI-Broker aus, das Einbinden von externen Systemen bleibt jedoch sehr aufwendig.

Das heute gültige Integrationskonzept des Enterprise Service Bus (ESB) enthält etablierte Standards wie MOM, Webservices und XML und besteht aus mehreren Einzelteilen. Die Grundkonzepte und die Notwendigkeit eines ESB lassen sich anhand eines beispielhaften Serviceprozesses verdeutlichen (siehe Kasten „Arbeit für den ESB). Der „Bus“ selbst ist meist eine MOM, die einen Nachrichtenkanal bereitstellt. Sie unterstützt Konzepte wie Request/Reply sowie synchrones und asynchrones Messaging und stellt sicher, dass die Nachrichten ihr Ziel unbeschadet erreichen.

## Immer gut informiert

Message Router gelten als wesentlicher Bestandteil einer ESB-Infrastruktur. Sie leiten die Nachrichten an einen oder mehrere Empfänger weiter. Die bekanntesten Vertreter, die Content-based Router, stellen Nachrichten abhängig vom Inhalt zu. Ein Filter ist ein spezieller Router, der Nachrichten untersucht und dafür sorgt, dass Servicekomponenten nur die für sie relevanten Neuigkeiten erhalten. Message Splitter teilen Nachrichten in mehrere Tranchen auf. Sie lassen sich beispielsweise so einstellen, dass sie nur Teile des Service Request an das Support Center weiterleiten. Beim Zusammenführen der Abschnitte hilft ein Message Aggregator.

Transformatoren wandeln Nachrichten von einem Format in ein anderes um. Beispielsweise muss eine JMS-Nachricht (Java Message Service)

**iX-TRACT**

- Integrationskonzepte wie Batch-Verarbeitung, Systemverbindungen über Konnektoren und File-Transfer sind in vielen Anwendungsszenarien nicht mehr zeitgemäß.
- Auf gängigen Standards basierende Enterprise-Service-Busse sind die modernen Vertreter der Softwarespezies für das Zusammenführen von Unternehmensanwendungen.
- Die Open-Source-Szene hat einsatzfähige ESB-Produkte zu bieten, etwa Mule, Service Mix, ActiveMQ und Camel.

## Arbeit für den ESB

Ein Unternehmen vermietet Kopierer und Büromaschinen. Die Kunden haben Serviceverträge abgeschlossen. Hat ein Kunde ein Problem mit einem Gerät, erfasst er dies über ein elekronisches Formular. Die Störungsmeldung wird an ein Messaging-System beim Anbieter weitergeleitet, das an den Enterprise Service Bus (ESB) angeschlossen ist. Sobald eine neue Nachricht eintrifft, startet der zuständige Service. Der Kunde erhält ein Support-Ticket sowie eine Auftragsbestätigung per E-Mail. Die Serviceabteilung analysiert zunächst die Beschwerde. Gängige Störungen kann der Bearbeiter oft telefonisch beheben. Handelt es sich um einen schwerwiegenden Fehler, muss sich ein Servicetechniker zum Ort des Geschehens begeben.

Er erhält eine SMS mit dem Termin sowie eine E-Mail mit allen notwendigen Informationen zum Servicefall. In diesem einfachen Prozess sind schon etliche Systeme beteiligt (Messaging, E-Mail, SMS, Unternehmensanwendung), die über den ESB zusammenarbeiten müssen.

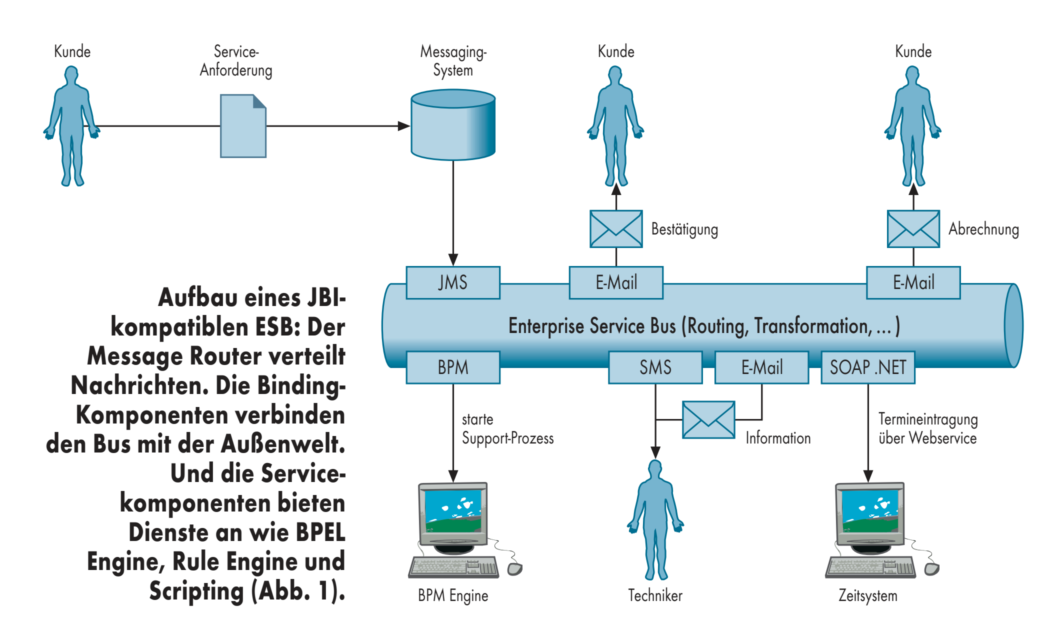
zum Weiterverarbeiten in ein XML-Dokument überführt werden. Der ESB bietet die Möglichkeit, Transformatoren in Serie zu schalten, um so mehrere Wandlungen sequenziell durchzuführen. Das Ergebnis des einen dient als Input des jeweils nächsten. Endpunkte (endpoints) verbinden Anwendung und Nachrichtenkanal. Jeder ESB-Hersteller stellt dafür eine API zur Verfügung, die die zu integrierenden Systeme implementieren müssen – es sei denn, sie sind über Webservices oder JMS ansprechbar. Entscheidend ist, dass der ESB über eine standardisierte Schnittstelle kommuniziert und nicht mit der applikationsspezifischen.

Es gibt mittlerweile viele kommerzielle und freie ESB-Produkte, die auf unterschiedlichen Konzepten basieren. Der Java-Business-Integration-Standard (JBI) versucht, die wesentlichen Funktionen zu vereinheitlichen. Über eine Komponentendefinition will er zusätzlich die Austauschbarkeit von Service- und Binding-Modulen erleichtern (Abbildung 1).

## Open Source für Profis

JBI legt fest, wie solche Komponenten zu beschreiben sind (im Wesentlichen mit der Web Services Definition Language, WSDL), und wie man sie zur Laufzeit einrichten und verwalten muss (über Java Management Extensions, JMX). Ein JBI-kompatibler ESB ist beispielsweise für das Lifecycle-Management der Komponenten verantwortlich. JBI ist ein einigermaßen schlanker Standard, der sich anderer Spezifikationen wie WSDL oder JMX bedient. Ziel ist es, dass sich JBI-Komponenten (Binding- wie Servicekomponenten) in verschiedenen ESB-Implementierungen gleichermaßen einsetzen lassen.

In fast allen Middleware-Installationen sind Clustering und Failover eine komplexe Angelegenheit. Trotzdem bieten auch Open-Source-Systeme entsprechende Funktionen. Man muss zwischen Clustering/Failover auf Broker- und Clientseite unterscheiden: Apaches Message Broker ActiveMQ beispielsweise erlaubt das Clustern von Nachrichtenkonsumenten (Clients). Das heißt, Nachrichten, deren Zustellung der Adressat nicht bestätigt, werden erneut geschickt und schnelle Clients erhalten mehr Nachrichten als langsame. Diese Mechanismen sind besonders dann interessant, wenn es gilt, viele Nachrichten zu verarbeiten, und ein einzelner Server dies




**Aufbau eines JBI-kompatiblen ESB: Der Message Router verteilt Nachrichten. Die Binding-Komponenten verbinden den Bus mit der Außenwelt. Und die Service-komponenten bieten Dienste an wie BPEL Engine, Rule Engine und Scripting (Abb. 1).**

nicht schafft. Zudem funktioniert diese Konstruktion auch als Failover-Setup, für den Fall, dass einzelne Clients ausfallen.

Das Failover und Clustering des Brokers ist wesentlich komplizierter. ActiveMQ bietet dafür trotzdem einige Optionen an, etwa das Failover-Protokoll für Sender. Ein Client kann darin mehrere Ziel-Broker angeben. Erreicht er den primären Server nicht, versucht er es mit dem jeweils nächsten auf seiner Liste – so lange, bis er seine Nachricht erfolgreich abgesetzt hat. Dies lässt sich mit einer dynamischen Suche nach Brokern kombinieren. Vorteil: Der Client muss nicht alle Broker-Adressen kennen. Eine Store-and-Forward-Konfiguration über mehrerer Broker lässt sich ebenfalls einrichten. Ein Broker kann darüber Nachrichten, für die er selbst nicht zuständig ist, an andere weiterreichen. Für den Failover-Fall kann man ein „Network of Brokers“ festlegen. Hier gibt es mehrere Optionen: Master/Slave mit manuellem Wiedereinfügen des Masters beim Failover, Master/Slave über ein Shared-File-System/Storage Area Network (SAN) (oder JDBC statt SAN). Auch wenn die Installation eines ActiveMQ-Servers für den Testbetrieb einfach ist: Für die Konfiguration eines Broker-Clusters mit Failover-Mechanismen braucht man einen Experten.

Im Open-Source-Umfeld haben sich in den letzten Jahren einige interessante Integrationsprojekte entwickelt. Dazu gehört ein ESB namens Mule, der unter Entwicklern zahlreiche Anhänger gewinnen konnte. Das inzwischen gegründete Unternehmen Mulesource erweiterte die Produktpalette rund um den ESB, der nun in einer Community- und in einer kommerziellen Enterprise-Ausführung existiert. Darüber hinaus bietet die Firma eine SOA-Governance-Plattform namens Galaxy an, zusätzlich das Managementwerkzeug Saturn sowie das Monitoring-Programm Mule HQ.

| Onlinequellen | |
|---|---|
| Mule ESB | mule.mulesource.org |
| Service Mix | servicemix.apache.org |
| Camel | activemq.apache.org/camel/ |
| ActiveMQ | activemq.apache.org |
| SEDA | www.eecs.harvard.edu/~mdw/proj/seda/ |

ESB-Produkte sind in der Regel komplex, was viele Softwarearchitekten und Entwickler erst mal abschreckt. Mule hingegen gibt sich unkompliziert, ist trotzdem flexibel und unterstützt zahlreiche Standardprotokolle. Version 2 basiert vollständig auf Spring 2.5 und kann deshalb auf wichtige Funktionen des Framework zurückgreifen, etwa Dependency Injection, AOP (Aspect Oriented Programming) und Transaktionsmanagement. Rund um Mule entstehen zahlreiche Zusatzprojekte, zum Beispiel ein SAP-Konnektor, ein Extended-XML- sowie ein Excel-Modul. Diese Erweiterungen lassen sich bei Bedarf ohne großen Aufwand anflanschen. Durch das modulare Konzept bleibt der Kern von Mule schlank (Abbildung 2).

## Kommunikation ist alles

Mule ESB stellt zahlreiche Konnektoren, Protokolle, Router, Filter, Transformatoren und Endpunkte zur Verfügung. Welche Artefakte geladen werden sollen, legt der Administrator wahlweise über eine XML-Konfiguration oder direkt über die API fest. Der Server besteht aus Containern, die die Servicekomponenten verwalten. In einem Container können beliebig viele Komponenten sowohl untereinander als auch mit externen Applikationen beziehungsweise Systemen kommunizieren.

Die Standardkommunikation basiert auf der Staged Event Driven Architecture (SEDA, siehe Kasten „Onlinequellen“ sowie *iX*-Link am Textende). Bei diesem Architekturpattern unterhalten sich die Komponenten über Event Queues. Alle Servicekomponenten verfügen über Endpunkte, mit denen Mule Nachrichtenkanäle aufbaut. Über die Endpunkte lassen sich alle Komponenten eindeutig identifizieren und ansprechen. Wie jedes ESB-Produkt läuft Mule auf einer MOM und benötigt somit kein angepasstes Umfeld. Mule wird mit einem Standard-Virtual-Machine-Protokoll ausgeliefert, das man als Message Broker einsetzen kann. Es bietet synchrone und asynchrone Kommunikation. VM-Queues lassen sich erhalten, was eine Kommunikation zwischen Komponenten auf VM-Ebene erlaubt. ActiveMQ kann hier als MOM arbeiten.

Der Nachrichtenfluss gliedert sich in die Phasen Inbound Flow, Component Flow und Outbound Flow Stage. Inbound Flow beginnt an den Endpunkten, die es ermöglichen, Servicekomponenten über zugewiesene Adressen anzusprechen. Die Inbound Router filtern, trennen oder führen bei Bedarf eingehende Nachrichten zusammen. Interzeptoren lassen sich sowohl davor als auch danach schalten, um die Komponente mit Querschnittsfunktionen (etwa Logging, Transaktionsmanagement, Sicherheit) zu erweitern.

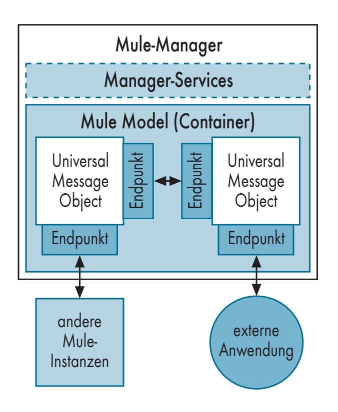
Nach dem Umwandeln der Nachricht in ein für die Komponente verständliches Format wird die Komponente ausgeführt (im Component Flow). Danach beginnt der optionale Outbound Flow Stage, beginnend mit dem Outbound Router, der die Nachricht weiterleitet. Mule implementiert einen Großteil der Enter-

prise Integration Pattern, wie sie Gregor Hohpe und Bobby Woolf in ihrem Standardwerk vorschlagen [1]. Anders als der Konkurrenz-ESB Apache Service Mix kümmert sich Mule direkt um deren Einrichtung. Service Mix lagert diesen Teilbereich an Apaches Integrations-Framework Camel aus.

## Gut sortiert: Gemischte Dienste

Letztes Jahr hat sich im Umfeld von ActiveMQ einiges getan: Service Mix startete als eine der ersten freien JBI-Implementierungen. Der modular aufgebaute ESB konzentriert sich auf die Komponenten-Infrastruktur, nicht auf bestimmte Services. Integration Patterns, Workflow Engines, Rule Engines und anderes mehr kann der Entwickler als Servicekomponenten hinzufügen. Die Administration erfolgt wie von JBI spezifiziert über JMX. Über die Java Management Extension lassen sich die Komponenten auch zur Laufzeit konfigurieren. Service Mix kann stand-alone oder in einer J2EE-Umgebung laufen. Bei Bedarf arbeiten ESBs zusammen, beispielsweise Mule mit Service Mix. Letztere Software kooperiert ebenso mit ActiveMQ und bildet so etwas wie den Klebstoff zwischen nachrichtenorientierter Middleware und Produkten wie Apache Camel.

Camel ist ein auf Spring aufsetzendes Integrations-Framework, das den Entwickler bei der Implementierung vieler Enterprise Integration Patterns hilft und sich dabei ebenfalls an den Ideen von Hohpe und Woolf orientiert. Es bietet die Möglichkeit, entweder über eine Java DSL (Domain Specific Language) oder eine XML-Konfiguration eine ganze Reihe von Patterns abzubilden (etwa Content-based Routing, Splitter, Content Enricher, Content Filter). Auf der Homepage des Produkts liegt eine




**Für Mule existieren zahlreiche Zusatzprojekte, die sich als Plug-in einfügen lassen (Abb. 2).**

Übersicht dazu. Das Werkzeug lässt sich einzeln betreiben oder als JBI-Komponente zum Beispiel in Service Mix einrichten. Dort würde es seinen Dienst als Servicekomponente verrichten. ActiveMQ Version 5 enthält Camel bereits. Interessant ist die Kombination der drei beschriebenen Projekte auch deshalb, weil sie aus demselben Entwicklerumfeld stammen. Zumindest verspricht das Zukunftsfähigkeit, Interoperabilität und guten Support. (jd)

DI MAG. MARKUS DEMOLSKY

arbeitet als Software Engineer und Berater bei der Soreco Group.

DR. ALEXANDER SCHATTEN

ist Assistent am Institut für Softwaretechnik und interaktive Systeme der TU Wien.

## Literatur

[1] Gregor Hophe, Bobby Wolf; Enterprise Integration Patterns; Designing, Building and Deploying Messaging Solutions; Addison-Wesley, 2004


iX-Link ix0807120





Kreditkartenindustrie verlangt Sicherheitsmaßnahmen

# Schutzzwang

**Randolf Skerka, Manuel Atug**

Seit Langem schon doktert die Kreditwirtschaft an verbindlichen Sicherheitsmaßnahmen für Unternehmen, die Kartendaten von Zahlungssystemen verarbeiten, herum. Jetzt ist Schluss mit lustig: Vehement fordern Kreditkartenanbieter die Umsetzung des Standards PCI DSS und verhängen immer häufiger Strafen bei Unterlassung.

Liest man die Schlagzeilen eines IT-Newstickers, muten die Meldungen an wie aus einem Cyberkrimi: Dem US-Einzelhändler TJX werden, wie die Öffentlichkeit im März 2007 erfährt, über einen Zeitraum von anderthalb Jahren über 90 Millionen Kreditkartendaten gestohlen, die Bilanz des börsennotierten Unternehmens weist hierfür im ersten Quartal 2008 250 Mio. US-$ Rückstellungen aus. Im April 2007 wird der Server des Softwareherstellers Valve kompromittiert und mehrere Tausend Kreditkartennummern geraten in die Hände der Eindringlinge. In Deutschland waren im Oktober 2007 über 60 000 Kunden des Online-Tickethändlers Kartenhaus vom Kreditkartendatendiebstahl betroffen. Und schließlich wird selbst das britische Militär im Januar 2008 Opfer eines Diebstahls privater Informationen mehrerer Hunderttausend Rekruten.

Für den Handel mit gestohlenen Kreditkartendaten hat sich mittlerweile ein reger Schwarzmarkt entwickelt. Nach Informationen des LKA Baden-Württemberg erzielen die Daten einer einzelnen Kreditkarte Preise zwischen 50 und 150 Euro. Für die Betroffenen ist der Schaden ungleich höher. Man kann davon ausgehen, dass pro missbräuchlich genutzter Kreditkarte ein durchschnittlicher Schaden von zwei- bis dreitausend Euro entsteht, bevor die Bank die Karte sperrt.

## Direkte und indirekte Schäden

Dementsprechend hoch sind die Schadenersatzanforderungen, denen sich ein Unternehmen im Schadensfall gegenüber sieht. Bei nur 3000 Kreditkartentransaktionen im Monat sammelt sich während der üblichen Gültigkeitsdauer von drei Jahren ein Datenschatz von 120 000 Kreditkartensätzen an. Damit beträgt allein der durch den Missbrauch der Karten direkt entstandene Schaden geschätzte 240 Millionen Euro. Dabei sind die Kosten für neu zu emittierende Kreditkarten, Rechtsstreitigkeiten und den gravierenden Imageschäden noch nicht berücksichtigt.

Der Schutz von Karteninformationen ist für jedes Unternehmen deshalb schon aus Eigeninteresse von höchster Priorität. Zusätzlich verlangen die Anbieter internationaler Zahlungssysteme – darunter MasterCard und Visa – die Umsetzung des Payment Card Industry Data Security Standard (PCI DSS) von allen Unternehmen, die Kartendaten der internationalen Zahlungssysteme verarbeiten, speichern oder weiterleiten. Dies sind unter anderem E-Commerce-, sogenannte MoTo- (Mail order/ Telephone order) und „klassische“ POS-Händler (Point of Sale) sowie deren Service Provider, etwa Webhoster, Payment Service Provider, Rechenzentrumsbetreiber, Fraud-Management-Dienstleister, Acquirer, Issuer und Prozessoren.

Die Einhaltung des Standards ist für alle verbindlich, ob großer oder kleiner Händler oder Service Provider. Aller-

**iX-TRACT**

- Wer Kartendaten der internationalen Zahlungssysteme Visa & Co. verarbeitet, speichert oder weiterleitet, ist zur Einhaltung des Sicherheitsstandards PCI DSS verpflichtet.
- Die Nachweise für die Umsetzung – externe Audits oder Selbsterklärung – hängen vom Transaktionsvolumen ab. Service Provider etwa müssen zwingend akkredierte Auditoren beauftragen.
- Wer den Standard nicht einhält, muss im Schadensfall mit erheblichen Vertragsstrafen und Schadensersatzforderungen rechnen.

dings unterscheidet der Standard die Zertifizierung, die sogenannte Compliance Validation, nach verschiedenen Händler- und Service-Provider-Abstufungen (Level). Nur Händler Level 1 (mehr als 6 Mio. Kartentransaktionen im Jahr von MasterCard oder Visa, oder mehr als 2,5 Mio Kartentransaktionen im Jahr von Amex) und Service Provider müssen die Einhaltung durch ein PCI DSS Security Audit und vier PCI DSS Security Scans im Jahr nachweisen. Bei kleineren Händlern reichen als Nachweis die Beantwortung eines PCI DSS Self-Assessment Questionnaire sowie die Durchführung von vier PCI DSS Security Scans im Jahr.

## Unterschiedliche Fristen je Anbieter

Große Level-1-Händler dürfen wahlweise das PCI DSS Security Audit intern durchführen, Service Provider müssen allerdings immer einen akkreditierten Auditor damit beauftragen. Security Scans dürfen ausschließlich akkreditierte Scan-Dienstleister durchführen.

Die Fristen, bis wann die Einhaltung durch erfolgreiche Zertifizierung nachzuweisen ist, geben die Zahlungssystemeanbieter im Rahmen ihrer PCI-DSS-Compliance-Programme unterschiedlich vor. Die Programme sind im Einzelnen:

- American Express: Data Security Operating Policy (DSOP)
- Discover: Discover Information Security Compliance (DISC)
- JCB: Data Security Program
- MasterCard: Site Data Protection (SDP)
- Visa USA: Cardholder Information Security Program (CISP)
- Alle anderen Visa-Regionen: Account Information Security (AIS)

Einige Fristen sind bereits verstrichen, andere laufen bald aus. Der Nachweis bei allen Service-Providern nach Visa AIS beispielsweise war bis spätestens 30. Juni 2005 zu erbringen. MasterCard SDP schreibt ebenfalls vor, dass Händler Level 1 und 3 (die Level definieren sich je nach Anzahl der Transaktionen pro Jahr) bis spätestens 30. Juni 2005 den Nachweis erbringen mussten, Händler Level 2 erhielten von MasterCard aufgrund einer Anpassung der Leveldefinition Aufschub bis 31. Dezember 2008.

Darüber hinaus gibt es immer wieder Ergänzungen und Präzisierungen, die zum Teil einen eigenen Stichtag haben – etwa die jüngste Erweiterung des PCI DSS im Bereich „Entwicklung und Wartung sicherer Systeme und Anwendungen“ (Requirement 6.6): Die auf Webapplikationen gemünzte Anforderung schreibt vor, diese vor bekannten Angriffen zu schützen – sei es durch Codereviews oder spezielle Web Application Firewalls. Zum 30. Juni 2008 wird aus dieser bislang empfohlenen Best-Practice-Maßnahme verbindliche Pflicht. Fachleuten zufolge ist das im April hierzu veröffentlichte Dokument „Information Supplement: Requirement 6.6 – Code Reviews and Application Firewalls Clarified“ auf den Webseiten des PCI SSC allerdings entgegen der eigentlichen Intention wenig präzise und teilweise missverständlich verfasst.

Schon 2000 beziehungsweise 2001 haben MasterCard und Visa angesichts der steigenden Missbrauchsraten im Umfeld von Kartentransaktionen die Programme MasterCard SDP und Visa AIS ins Leben gerufen, um die Sicherheit von Kartendaten bei der Verarbeitung, Speicherung und Weiterleitung zu gewährleisten.

Ende 2004 (MasterCard) bis Anfang 2005 (Visa) haben die Verantwortlichen die bis zu diesem Zeitpunkt voneinander unabhängigen technischen Anforderungen in den PCI DSS zusammengeführt, den der Payment Card Industry Security Standards Council (PCI SSC, www.pcisecuritystandards.org) seitdem weiterentwickelt. Neben MasterCard Worldwide und Visa Inc sind American Express, Discover Financial Services und JCB International weitere Gründungsmitglieder.

Im September 2006 wurde der Standard selbst und im Februar 2008 auch der Selbstbewertungsfragebogen (Self-Assessment Questionnaire) überarbeitet. Der PCI DSS setzt sich derzeit zusammen aus dem eigentlichen Standard, dem Fragebogen, Sicherheitsscans und -audits sowie neuerdings einer Softwarevalidierung:

- PCI Data Security Standard, Version 1.1
- PCI DSS Self-Assessment Questionnaire, Version 1.1
- PCI DSS Security Scanning Procedures, Version 1.1
- PCI DSS Security Audit Procedures, Version 1.1
- PCI Payment Application Data Security Standard, Version 1.1

## Vereinfachungen für Anwender

Im April 2008 wurde das von Visa vormals als Visa Payment Application Best Practices veröffentlichte Softwareprüfverfahren unter dem Namen PCI Payment Application Data Security Standard (PA-DSS) eingegliedert. Dieser stellt eine Ableitung eines „Software-Standards“ aus dem PCI Data Security Standard dar, dessen Ziel es ist, den Anwender durch Einsatz der Software beim Einhalten des PCI DSS zu unterstützen.

Das PABP-Zertifizierungsschema läuft zum Ende September aus. Ab Oktober ist Software daher ausschließlich nach dem neuen PA-DSS zu prüfen. Neu im PA-DSS ist, dass im Standard und den begleitenden Dokumenten darauf hingewiesen wird, dass eine Überarbeitung durch das PCI SSC im Zweijahreszyklus erfolgen wird, was sowohl die Planungs- und Investitionssicherheit als auch Release-Wechsel und darauf resultierende Migrationsplanungen bei Softwareherstellern, Integratoren und Kunden erleichtert. Gleiches ist zukünftig auch für den PCI DSS angekündigt.

Da der PA-DSS von Visa in den USA bereits in fünf vorgeschriebenen Schritten bis zum Jahr 2010 verpflichtend wird, ist auch in Europa die Verpflichtung zur ausschließlichen Nutzung von zertifizierter Payment-Software in naher Zukunft zu erwarten.

Für Oktober 2008 hat der PCI SSC eine überarbeitete Fassung des PCI DSS angekündigt. Council-Mitglieder und akkreditierte Partner erhalten einen Entwurf der neuen Fassung zur Kommentierung circa 45 Tage vorab.

Zusätzlich zu den frei verfügbaren Standards hält die Webseite des PCI SSC weiteres Material bereit, etwa den PCI DSS in verschiedenen weiteren Sprachen – zum Beispiel Deutsch, Französisch und Spanisch –, aber auch Interpretationsunterstützungen wie das Dokument „Navigating PCI DSS – Understanding the Intent of the Requirements“ sowie ein Glossar.

Wer im Falle der Kompromittierung von Kartendaten nicht nachweisen kann, den Anforderungen dieses Standards genügt zu haben, riskiert empfindliche Vertragsstrafen und Schadensersatzanforderungen. Im Gegenzug gewähren die Kreditkartengesellschaften eine teilweise oder vollständige Befreiung von

### Organisatorische Kernpunkte

- geregeltes Change-Management
- anerkanntes Key-Management
- sorgfältige Systemdokumentation
- Genehmigungsprozesse
- Sicherheitskonzepte

den vertraglichen Strafzahlungen („Safe Harbor Rule“), wenn sie den Standard zum Zeitpunkt der Kompromittierung als voll erfüllt ansehen und eine Zertifizierung durchgeführt wurde.

Allgemein gesprochen befasst sich der PCI DSS mit dem Schutz von Kreditkartendaten. Dafür bedient er sich zwölf übergeordneter Anforderungen („Requirements“; siehe Kasten „Die zwölf Anforderungen …“), die sich jeweils einem spezifischen Aspekt der Sicherheit von Kartendaten widmen. Jedes übergeordnete Requirement enthält eine Reihe konkreter Handlungsanweisungen, die für eine Zertifizierung ausnahmslos zu erfüllen sind. Dabei sind technische Sicherheitsanforderungen auf Netzwerk-, System- oder Applikationsebene ebenso enthalten wie organisatorische und personelle Maßnahmen zum Erreichen sicherer Geschäftsprozesse im Umgang mit Kartendaten (siehe Kasten „Organisatorische Kernpunkte“).

## Technischer Schutz allein genügt nicht

Damit wollen die Verantwortlichen dem Umstand Rechnung tragen, dass eine ausschließlich technische Lösung heutzutage keine ausreichende Sicherheit mehr bieten kann. Selbst bei Einsatz der besten Firewalls ist jedes System im Zweifelsfalle nur so sicher wie das schwächste Passwort, das seine Nutzer verwenden. Auf den ersten Blick mag dies übertrieben klingen, doch mithilfe von im Internet frei verfügbaren Hackingtools lassen sich kleinste Schwachstellen wie ein nachlässig gewähltes Passwort oder ein fehlendes Sicherheits-Update auch durch relativ ungeübte Hacker leicht und schnell ausnutzen, um Zugriff auf ein ansonsten sicheres System zu erlangen.

Deshalb setzt der PCI DSS auf eine tiefgreifende Verwurzelung der Sicherheitsmaßnahmen in den Systemen selbst: Diese sind so zu konfigurieren, dass beispielsweise das Wählen unsicherer Passwörter grundsätzlich ausgeschlossen wird. Daneben ergeben sich durch eine PCI DSS-Zertifizierung tiefschürfende Änderungen in einer ganzen Reihe unterschiedlichster Unternehmensprozesse, von denen sich viele nicht auf die IT-Abteilung beschränken lassen.

So fordert der Standard unter anderem einen hinreichenden Zugriffsschutz von Kartendaten, was neben der möglichst restriktiven Verteilung von Zugriffsrechten in Computersystemen auch die Einführung von offen zu tragenden Mitarbeiterausweisen oder die Installation von Videokameras und Zugangskontrollen mit sich bringt.

## Auswirkungen im Tagesgeschäft

Obgleich sich ein Großteil der Änderungen für die meisten Nutzer weitgehend unbemerkt in die Sicherheitsarchitektur der IT-Landschaft integrieren wird, haben einzelne Anforderungen des PCI DSS spürbare Auswirkungen auf das Arbeiten im Tagesgeschäft. Nicht alle dieser Änderungen werden das Arbeiten erleichtern, einige betreffen liebgewonnene Abläufe. Doch alle vom PCI DSS geforderten Maßnahmen sind notwendig, um den Schutz der Kartendaten sicherzustellen und den Fortbestand und das Vertrauen in die Zahlungssysteme zu gewährleisten.

Die Zahlungssystemanbieter teilen Händler und Service Provider nach Transaktionsvolumen oder Art der Dienstleistung in unterschiedliche Level ein. Die Händlerklassifizierung von MasterCard und Visa sowie die Service-Provider-Klassifizierung der beiden sind im Detail verfügbar (siehe *iX*-Link), weniger ausführliche Informationen gibt es auch bei anderen Zahlungssystemen. Händler können das PCI DSS Security Audit intern durchführen.

Die Bewertung (Compliance Validation) von PCI DSS Security Scans sowie bei Service-Providern durchzuführenden PCI DSS Security Audits erfolgt ausschließlich durch akkreditierte Partner (PCI Approved Scanning Vendor beziehungsweise PCI Qualified Security Assessor) des PCI Security Standards Council.

Weder Händler noch Service Provider werden sich dem PCI DSS langfristig entziehen können. Insbesondere MasterCard und Visa, aber neuerdings auch American Express fordern den Nachweis zur Einhaltung des PCI DSS immer vehementer ein. Auch sprechen die Anbieter inzwischen immer häufiger Vertragsstrafen in Form von Penalen zur Nichteinhaltung des PCI DSS aus.

Der Payment Card Industry Security Standards Council hat den PCI DSS über die Jahre mehrfach überarbeitet. Entstanden ist ein ganzes Framework, das wohl auch zukünftig an neue Bedrohungen und Risiken angepasst werden wird – wie kürzlich durch die Einführung des Payment Application Data Security Standard (PA DSS) geschehen. Neben bereits etablierten Sicherheitsstandards wird sich der PCI DSS langfristig einen Platz sichern. (ur)

RANDOLF SKERKA UND MANUEL ATUG

sind Berater bei SRC Security Research Consulting in Bonn.





## Die zwölf Anforderungen des PCI DSS

**1. Einrichtung und Unterhaltung eines sicheren Netzwerks**

Anforderung 1: Installation und Verwaltung einer Firewall-Konfiguration zum Schutz von Karteninhaberdaten

Anforderung 2: Keine Verwendung der Standardwerte des Herstellers für Systemkennwörter und andere Sicherheitsparameter

**2. Schutz von Karteninhaberdaten**

Anforderung 3: Schutz von gespeicherten Karteninhaberdaten

Anforderung 4: Verschlüsselung der Übertragung von Karteninhaberdaten über offene, öffentliche Netzwerke

**3. Verwalten eines Programms zur Bewältigung von Sicherheitsrisiken**

Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirusprogrammen

Anforderung 6: Entwicklung und Verwaltung sicherer Systeme und Anwendungen

**4. Implementieren strikter Zugriffssteuerungsmaßnahmen**

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten auf die geschäftlich erforderlichen Daten

Anforderung 8: Zuweisung einer eindeutigen ID zu jeder Person mit Computerzugriff

Anforderung 9: Beschränkung des physischen Zugriffs auf Karteninhaberdaten

Anforderung 10: Protokollieren und Prüfen aller Zugriffe auf Daten von Kreditkarteninhabern

**5. Regelmäßiges Überwachen und Testen von Netzwerken**

Anforderung 11: Regelmäßiger Test von Sicherheitssystemen und -prozessen

**6. Verwalten einer Informationssicherheitsrichtlinie**

Anforderung 12: Verwaltung einer Informationssicherheitsrichtlinie für Mitarbeiter und beauftragte Unternehmen

Anwendungsentwicklung für den Blackberry

# Rein in die Firma

**Jochen Kokemüller, Michael Schäfer**

Der mobile Zugriff auf Unternehmensanwendungen spielt eine immer wichtigere Rolle. Wer seinem Blackberry einen Pfad in die Firma öffnen will, sollte sich RIMs Entwicklungsumgebung MDS-Studio ansehen.



Heutzutage gehört E-Mail zu den üblichen Funktionen eines geschäftlich genutzten mobilen Endgerätes. Zusätzlichen Nutzen bringt der Zugriff auf Anwendungen im Intranet des Unternehmens. Research in Motion (RIM) setzt hierfür auf serviceorientierte Architekturen (SOA). Die HTTP-Verbindung läuft über RIMs Network Operating Center (NOC) direkt in das Intranet des Unternehmens, wo der Blackberry Enterprise Server (BES) als Brückenkopf fungiert.

Es gibt drei Varianten der Software für Blackberries: im Browser laufende Webanwendungen, Java-Applikationen und die per MDS-Studio erstellten Programme, die eine Zwischenstellung einnehmen. Um sie geht es im Folgenden. Die Windows-IDE ist als kostenfreier 232 MByte großer Download bei RIM erhältlich (siehe *iX*-Link).

Dieser Artikel beschreibt das Erstellen einer Anwendung, die via Webservices auf eine Veranstaltungsliste zugreift. Anwender können damit Veranstaltungen direkt buchen; die Termine und Kontakte überträgt der Webservice automatisch in das Gerät und versendet eine E-Mail an den Veranstalter.

Beim Anlegen eines neuen Projekts in MDS-Studio stehen zwei Wizards zur Verfügung. Der „Quick Start Approach Wizard“ erstellt aus den in der WSDL (Web Services Description Language) deklarierten Datenstrukturen eine Benutzungsschnittstelle und die elementaren Operationen zur Interaktion. Der „Bottom-Up Approach Wizard“ verzichtet auf die GUI und erzeugt nur die Nachrichten- und Datenkomponenten sowie deren Beziehungen zueinander. Um ihn geht es hier.

## Das Grundgerüst aus der WSDL

Auf seiner zweiten Seite erfragt der Wizard die URL zur WSDL. Sie lautet für das Beispiel

http://document.swm.iao.fhg.de:8000/Kalender/services/kalender?wsdl

Hat er die Schnittstelleninformation gelesen, muss man die Operationen *getEvents* und *getDetailsByID* auswählen. Der Projektname ist frei wählbar, beispielsweise „IAO Kalender“.

Im Navigator erscheint nun das Projekt mit den Teilen *Application* und *Data Sources*. Wesentlich für das Weitere sind die vier Kinder von *Application*: *Data, Messages, Screens* und *Scripts*. Bildschirme (Screens) enthalten Buttons, Labels oder Menüs und bilden die Benutzungsschnittstellen. Nachrichten (Messages) transportieren die zwischen Webservice und Client ausgetauschten Informationen. Lokale und globale Variablen sowie Bildschirmparameter speichern Daten (Data), die die unmittelbare Schicht zwischen Nachrichten und Bildschirmen bilden. Bildschirmparameter reichen Daten an Screens oder Scripts weiter. In Javascript geschriebene Scripts verarbeiten Benutzereingaben oder Ereignisse (Events) wie den Empfang einer Nachricht.

Der einzige vom Wizard erstellte Screen *scrMain* enthält anfangs nur einige Labels in einem Container, der Region. In diesem Screen soll der Anwender seine Suchabfrage formulieren und dazu den ihn interessierenden Zeitraum eingeben. Die Suchergebnisse bekommt er ebenfalls in *scrMain* tabellarisch angezeigt.

Im linken Teil von MDS-Studio liegt eine Toolbar, die Bildschirmelemente zum Hinzufügen per Drag & Drop bereithält. Zunächst sollte man jedoch alle vorhandenen Elemente entfernen. Eine neue Region mit dem Layout *Grid* ordnet die Elemente in zwei Spalten an. In ihr platziert man *EditBox*-Elemente

als Eingabefelder und die zugehörigen Beschriftungen (*Label*). Ein in den Attributen einer *EditBox* angegebenes Eingabeformat fängt eventuelle Tippfehler sofort ab. So sollten für ein Datum der Wert von *EntryType* auf *date* und das Format auf *dd.MM.yyyy* stehen. Neben den beiden Eingabefeldern für das Datum und ihrer Beschriftung enthält der Screen einen Button zum Abschicken. Beim Hinzufügen öffnet sich ein Popup-Menü zur Konfiguration des Buttons. Da die mit ihm verbundene Aktion erst später definiert wird, ist die Option „Define later“ zu wählen. Screens lassen sich mit Styles formatieren, die unter anderem Schrift und Farbe der Bildschirmelemente festlegen. Man fügt sie im Navigationsbereich dem Projekt hinzu.

Als Nächstes entsteht der Bildschirm für die Detailanzeige *scrDetails*. In seinem Eigenschaftsfenster legt man den neuen Parameter „details“ vom Typ *Details* an. Dieser Datentyp ist mit seinen Attributen in der WSDL definiert.

Jetzt können die Bildschirmeigenschaften um die Attribute der Klasse *details* erweitert werden. Um beispielsweise die Bildschirmeigenschaft „Titel“ automatisch zu setzen, bekommt sie das Attribut *titel* des Bildschirmparameters *details* zugewiesen. Nun steht „@details.titel“ in der Zeile des Screen-Titels (siehe Abb. 1).

## Anwendungsdaten reisen zum Server

Der nächste Schritt ist das Absetzen der Suchanfrage an den Server. Dafür soll der Button in *scrMain* eine Nachricht vom Typ *getEventsRequest* erstellen und zum Server schicken. Wenige Zeilen Javascript, mit dem *OnClick*-Ereignis des Buttons verbunden, weisen die Werte der Eingabefelder den Attributen der Nachricht zu und versenden diese:

```
getEventsRequest.parameters.in0 =
  scrMain.editBox1.value;
getEventsRequest.parameters.in1 =
  scrMain.editBox2.value;
getEventsRequest.send();
```

Die Antwort, ein Array mit dem Suchergebnis, soll die globale Variable *veranstaltungen* des Typs *Veranstaltung* speichern. Auch dieser Typ stammt aus der WSDL. Die Variable lässt sich unter „New Global…“ mit der Option *array = true* anlegen. Die Zuweisung der Werte erfolgt durch Doppelklick auf die Nachricht *getEventsResponse*: Unter dem Reiter „Fields“ lässt sich die gewünschte Zuweisung (Data Mapping) erstellen. Der Einzeiler *Screen.refresh()* im Event *onGetEventsResponse* der Nachricht stellt sicher, dass die Darstellung nach Erhalt der Nachricht dem aktuellen Stand entspricht.

Da das Suchergebnis ein Array ist, bietet sich seine Anzeige in einer Tabelle mit zwei Spalten an. Sie kann analog zu obigen Screen-Elementen in *scrMain* stehen, ihr Wert ist die Variable *veranstaltungen*. Die Spalten der Tabelle erhalten nun die Attribute wie *veranstaltungen.titel* und *veranstaltungen.datum* zugewiesen.

Zum Auswählen eines Tabelleneintrags dient ein *MenuItem*, dessen Eigenschaft *OnClick* das folgende Skript zugeordnet bekommt:

```
if (scrMain.table1.selectedRowIndex >= 0) {
  var veranstaltung = veranstaltungen[
    scrMain.table1.selectedRowIndex];
  getDetailsByIDRequest.parameters =
    veranstaltung.veranstaltungsid;
  getDetailsByIDRequest.send();
}
```

Es holt sich das in der Liste ausgewählte *Veranstaltung*-Objekt. Sein Feld *veranstaltungsid* enthält die ID des zugehörigen *Details*-Objekts, das die Anwendung mit der Nachricht *getEventByIDRequest* vom Webservice anfordert. In den Eigenschaften dieser Nachricht ist ein Skript hinterlegt. Es speichert das eingehende Objekt und übergibt es als Argument an einen anderen *Screen*:

```
var details = getEventByIDResponse.parameters;
scrDetails.display(details);
```

Dadurch öffnet sich *scrDetails* erst beim Eintreffen der Daten.

## Termin in den Kalender eintragen

Durch Gerätefunktionen lassen sich neue Einträge in den Kalender oder das Adressbuch übernehmen. Listing 1 zeigt den Code für das Eintragen einer Veranstaltung in den Kalender. *FREEBUSY* ist eine Enumeration mit den Werten *FREE, TENTATIVE, BUSY* (Voreinstellung) und *OUT_OF_OFFICE*. Damit das Gerät die neuen Daten speichert, muss in den Properties der aufrufenden Buttons beziehungsweise *MenuItems* die Option *Accept Changes* auf *commit* stehen.

**Listing 1: Hinzufügen eines Kalendereintrags**

```
var myEvent = Event.create();
if( myEvent != null ) {
  myEvent.start = param.beginn;
  myEvent.free_busy = FREEBUSY.TENTATIVE;
  myEvent.location = param.ort.name;
  myEvent.note = param.typ;
  myEvent.summary = param.titel;
  myEvent.allday = true;
}
```

Ähnlich einfach lässt sich ein Kontakt ins Adressbuch übernehmen:

```
var c = Contact.create();
c.nameGiven = param.verantwortlicher.vorname;
c.nameFamily = param.verantwortlicher.name;
c.Email1 = param.verantwortlicher.email;
c.workTel = param.verantwortlicher.telefon;
```

Zusätzlich zur Methode *create()* stehen für Termin- und Adress-Objekte die Methoden *findWhere()* sowie *removeAll()* zur Verfügung. Mit

```
Event.findWhere("start = 'Jan 1, 2009'")
```

lässt sich beispielsweise auf den nächsten Neujahrstag zugreifen. Listing 2 zeigt ein Skript, das in eine Nachricht die Telefonnummer und die E-Mail-Adresse des Benutzers einbaut und sie dann versendet. Damit sie die Daten aus dem Bildschirm *scrDetail* verwenden können, haben die Skripte jeweils einen Parameter namens *param* vom Typ *Details*.

### MDS-konforme WSDL-Dateien

MDS-Studio hat mit dem Import von WSDL-Dateien manchmal Schwierigkeiten. Zuverlässig funktioniert es, wenn die Daten folgende Bedingungen erfüllen:

– Konformität mit dem WS-I-Standard;

– Verzicht auf schwache Typen wie *<xs:any>* oder *<xs:union>*;

– Reduzierung der Datenmenge für den mobilen Einsatz etwa durch Verzicht auf Attribute;

– Verwendung statischer Daten wie Enumerationen, um Bandbreite zu sparen;

– Die Rückgabe langer Listen durch die Verwendung einschränkender Suchbegriffe vermeiden;

– Verzicht auf Rekursion und Schachtelung.

Lässt sich der Webservice nicht mehr ändern, kann man die API über einen Proxy-Webservice anpassen. Er bietet nach außen nur die Operationen und Typen an, die den oben genannten Kriterien genügen.

**Listing 2: Verfassen einer E-Mail**

```
var deviceinfo = DeviceInfo.create();
var mail = Message.create();
mail.toRecipients = param.verantwortlicher.email;
mail.subject = param.titel;
mail.content = Sehr geehrte(r) Herr/Frau " + params.verantwortlicher.name +
     "\nfür Ihre Veranstaltung möchte ich hiermit unverbindlich zusagen. " +
     "Telefonisch bin ich unter " + deviceinfo.phoneNumber + " zu erreichen. " +
     "Meine E-Mail-Adresse lautet " +
     mail.from +
     ".\nMit freundlichen Grüßen" +
     "\nDiese Mail wurde mit dem IAO Kalender für Blackberry automatisch generiert. ";
var status = mail.send();
if(status == Message.SENT) {
     Dialog.display("Die Mail wurde erfolgreich gesendet.");
```

MDS-Studio bietet eine einfache Möglichkeit zum Testen der Anwendung. Dafür wählt man „Test“ im Kontextmenü des Projekts. Zusammen mit der sich nun öffnenden Test-Perspektive lädt die IDE den Blackberry-Simulator, was auf langsamen Rechnern etwas dauern kann. Auf der simulierten Oberfläche befindet sich das Icon für die eigene Anwendung, die sich so ausgiebig testen lässt. Einen Debugger liefert RIM bislang allerdings nicht, es bleibt also nur das Einbauen von *Debug.write()*-Befehlen für die Fehlersuche.

## Der lange Weg auf den Blackberry

Nach dem Erstellen der Anwendung ist es an der Zeit, sie auf ein echtes Gerät zu übertragen. Im MDS-Studio steht generell nur das Deployment via BES zur Verfügung. Dafür muss man in den Einstellungen unter „Publishing“ die „Application Registry“ und das „File Repository“ angeben. Beide wurden bei der Installation des BES angelegt. Der im Kontextmenü des Projekts verfügbare „Publish Wizard“ stellt die Anwendung in der Application Registry zum Deployment bereit. Zum endgültigen Übertragen auf die Hardware muss der Administrator sie mit dem Blackberry Manager dem Gerät zuweisen. „Devices Registered“ führt dazu alle Blackberries auf, für die diese Zuweisung möglich ist.

Insbesondere muss auf dem Gerät die MDS-Runtime installiert sein. Dafür wird das Archiv mit der Runtime (siehe *iX*-Link) in dem freigegebenen Netzordner *Shared\Applications* auf dem BES-Server (gewöhnlich unter *C:\Programme\Gemeinsame Dateien\Research In Motion*\) entpackt. Durch Erneuern des Index mit dem Befehl *AppLoader/Loader.exe /reindex* erfährt der Server von der neuen Runtime.

Für die Übertragung der MDS-Runtime ist eine Softwarekonfiguration notwendig. Das ist eine Sammlung von einer oder mehreren gemeinsam auf den Endgeräten zu installierenden Anwendungen. Zu ihrer Erstellung dient wiederum der erwähnte Blackberry Manager. Seine Option „Policy“ legt unter anderem fest, ob die Anwendung für den Benutzer optional oder zwingend zu installieren ist, und ob sie auf seine persönlichen Daten (E-Mail-Adresse, Kontakte et cetera) zugreifen darf.

Im Blackberry Manager wird nun noch der Benutzer mit der Softwarekonfiguration verbunden. Sind alle Einstellungen vorgenommen, überträgt der BES die Anwendung auf das Gerät, was bis zu vier Stunden dauert. Ist die MDS-Runtime auf dem Endgerät installiert, muss der Benutzer sie durch einmaliges Starten aktivieren. Danach kann der Veranstaltungskalender drahtlos auf das Gerät übertragen werden.

## Fazit

Mit MDS-Studio lassen sich Webservices-Anwendungen einfach entwickeln. Mobile Software muss jedoch einige Anforderungen erfüllen, deren Einhaltung eine IDE alleine nicht garantieren kann. Große Grafiken etwa verstopfen die ohnehin knapp bemessene mobile Datenleitung. Verkleinert man sie, sind sie häufig nur noch schwer zu erkennen. Deshalb ist es häufig ratsam, auf Grafiken soweit wie möglich zu verzichten oder sie zumindest für den kleinen Bildschirm zu optimieren.

Da Anwender unterwegs oft wenig Zeit haben, muss die Navigation sie schnell und gezielt durch das Programm führen. Das bedeutet, dass sie in der Regel einfacher gestaltet sein muss als bei stationären Anwendungen und dass die Seite keinen überflüssigen Schnickschnack enthalten darf. Dazu gehört auch, Tabellen kompakt zu halten und sich auf wenige Spalten zu begrenzen sowie Scrollen zu vermeiden. Wer diese wenigen elementaren Punkte beherzigt, kann mit dem MDS-Studio effizient Unternehmensanwendungen mobil zur Verfügung stellen. Insbesondere, wenn schon eine SOA-Landschaft besteht. (ck)




**Der Detail-Screen *scrDetail* zeigt Attribute der Klasse *details* an. Sie ist in der WSDL-Datei definiert (Abb. 1).**


JOCHEN KOKEMÜLLER

ist als wissenschaftlicher Mitarbeiter am Fraunhofer Institut für Arbeitswirtschaft und Organisation (IAO) beschäftigt. Seine Schwerpunkte liegen in den Bereichen DMS, SOA und mobile Anwendungen.

MICHAEL SCHÄFER

studiert an der Universität Stuttgart Softwaretechnik. Zu seinen Kompetenzen zählt die Entwicklung mobiler Anwendungen und Webservices.



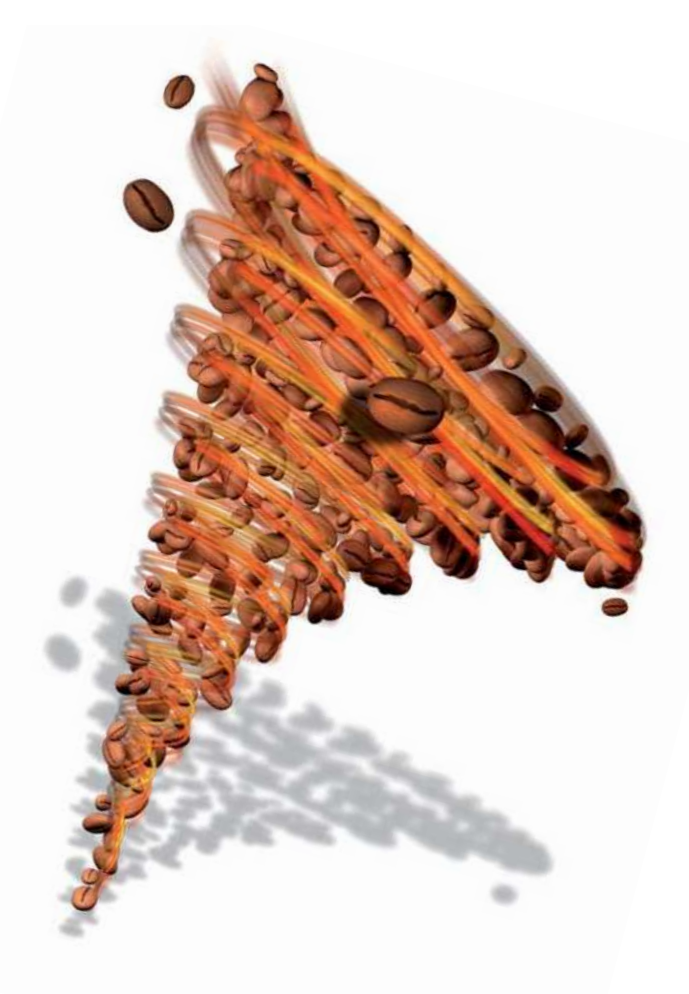




Mehr Komfort durch das neue Swing Application Framework

# In Schwung kommen

**Thomas Künneth**



Mit dem Swing Application Framework möchte Sun in der für Anfang nächsten Jahres erwarteten Java Version 7 das Erstellen von Programmen mit grafischer Benutzerschnittstelle radikal vereinfachen. Der schon verfügbare Prototyp macht Appetit auf die endgültige Fassung.

Eigentlich bringt Swing, der für das Erstellen von grafischen Benutzeroberflächen zuständige Teil der Java-Standardklassenbibliothek, alles mit, was für den Bau moderner und schöner Anwendungen notwendig ist. Allerdings oblag es bisher ausschließlich dem Entwickler, die unzähligen Bestandteile von Swing sinnvoll zu kombinieren. Dieses Verdrahten erfordert nicht nur eine große Menge an Infrastrukturcode, sondern auch viel Wissen um interne Zusammenhänge.

Nicht nur Einsteiger kämpfen beispielsweise zuweilen mit dem Phänomen, dass das Setzen einer Komponenten-Eigenschaft keinen sichtbaren Erfolg hat. Alte Hasen sorgen dafür, dass solche Aktionen im sogenannten Event Dispatching Thread (EDT) ausgeführt werden. Im Laufe der Zeit entsteht so eine Sammlung von Quelltextfragmenten, die der Programmierer in seinen Anwendungen einsetzt. Wenn solcher Code wieder und wieder implementiert werden muss, liegt es eigentlich nahe, ihn in den Standard zu übernehmen. Mit dem Swing Application Framework vollzieht Sun endlich diesen lange herbeigesehnten Schritt.

Im Mai 2006 hat Sun hierzu den Java Specification Request (JSR) 296 auf den Weg gebracht. Er beschreibt einen schlanken und leicht verständlichen Rahmen, der sich unter anderem um das Starten und Beenden von Swing-Anwendungen kümmert, die Verwaltung lokalisierter Ressourcen übernimmt, das automatische Setzen von Komponenteneigenschaften beherrscht sowie Sitzungen speichern und wiederherstellen kann.

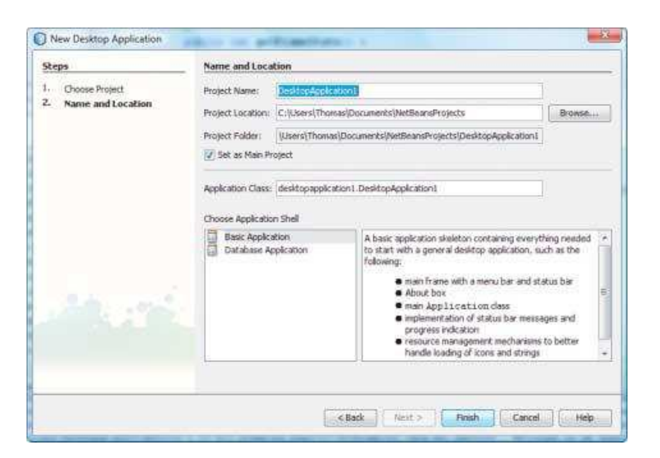
Diese Aufzählung verdeutlich, dass das Swing Application Framework nicht in Konkurrenz zu den großen Plattformen Netbeans RCP und Eclipse RCP tritt. Der Anspruch ist, eine leichtgewichtige Alternative zu bieten, die auch Einsteiger schnell in die Lage versetzt, kleine bis mittlere Anwendungen zu bauen. Ob dies gelingen kann, soll ein erster Blick auf den Prototyp zeigen. Mit der Version 7 von Java erwartet man die endgültige Fassung für Anfang nächsten Jahres.

**iX-TRACT**

- Das neue Swing Application Framework, das zurzeit als Prototyp verfügbar ist, soll Teil der für Anfang nächsten Jahres erwarteten Version 7 von Java sein.
- Indem es wiederkehrende Aufgaben wie das Starten und Beenden einer Anwendung übernimmt und unter anderem Komponenteneigenschaften automatisch setzt, erleichtert das Framework die Programmierung von Swing-Applikationen erheblich.
- Entwickler werden von unnötiger Schreibarbeit befreit und können ihre Anwendungen besser strukturieren.

## Aller Anfang kann auch leicht sein

Erhältlich ist der Prototyp auf der Community-Site appframework.dev.java.net. Von dort können Interessierte den Quelltext als Netbeans-Projekt, die bereits übersetzten Klassen sowie ein Archiv mit der Dokumentation herunterladen. Der Bau der Bibliothek gestaltet sich einfach. Anwender der Netbeans-IDE müssen nur das Projekt öffnen und




**Beim Anlegen einer Swing-Anwendung bietet das Framework dem Programmierer zwei Unterkategorien des Projekttyps „Java Desktop Application" an (Abb. 1).**

anschließend durch Anklicken von Build im Kontextmenü des Projekts den Build-Vorgang anstoßen.

Mittels „Generate Javadoc" im selben Menü lässt sich die Dokumentation generieren. Benutzer anderer Entwicklungsumgebungen legen einfach ein neues Projekt an und kopieren den Inhalt des Verzeichnisses *src* aus dem Archiv *AppFramework-1.03-src.zip* in den Standard-Quelltextordner des Projekts. Netbeans bringt ab der Version 6.0 das Swing Application Framework bereits mit. Die IDE unterstützt den Programmierer beispielsweise beim Anlegen einer Swing-Anwendung durch den neuen Projekttyp „Java Desktop Application". Er bietet die beiden Unterkategorien „Basic Application" und „Database Application".

Das Swing Application Framework steuert den Lebenszyklus einer Anwendung. Damit dies funktioniert, müssen Programme von *org.jdesktop.application.Application* ableiten und bestimmte Methoden überschreiben. Listing 1 zeigt ein erstes, einfach gehaltenes Beispiel.

**Listing 1**

```
package com.thomaskuenneth.appframework;
import java.awt.BorderLayout;
import javax.swing.JFrame;
import javax.swing.JLabel;
import org.jdesktop.application.Application;

public class Demo1 extends Application {
    public static void main(String[] args) {
        Demo1.launch(Demo1.class, args);
    }
    @Override
    protected void startup() {
        JFrame f = new JFrame(getClass().getName());
        JLabel label = new JLabel("Hallo iX");
        f.add(label, BorderLayout.CENTER);
        f.setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);
        f.pack();
        f.setLocationRelativeTo(null);
        f.setVisible(true);
    }
}
```

**Der Aufruf von *startup()* erfolgt implizit beim durch *launch()* ausgelösten Hochfahren der Anwendung.**

Es öffnet ein Fenster mit einem Label als einzige (sichtbare) Komponente. Der Bau der Oberfläche findet vollständig in der Methode *startup()* statt, deren Aufruf allerdings nicht direkt erfolgt. Stattdessen initiiert die statische Methode *launch()* der Klasse *Application* das Hochfahren der Anwendung. Im Zuge dessen erfolgt ein Aufruf von *startup()*.

## Listener entscheiden über Programmende

Das Schließen des Fensters führt hier zu einem sofortigen Programmende. Die Mechanismen, die das Framework zum kontrollierten Herunterfahren vorsieht, werden noch nicht genutzt. In Listing 2 öffnet ein Klick auf das Schließfeld des Fensters nun einen Dialog, den der Benutzer mit „Ja" bestätigen muss. In diesem Fall wird die Methode *exit()* der Klasse *Application* aufgerufen. Sie beginnt mit dem Herunterfahren der Anwendung. Der erste Schritt besteht darin, alle registrierten *ExitListener* über das bevorstehende Programmende zu informieren. Die Listener können den Vorgang gegebenenfalls abbrechen.

Listing 2 implementiert hierzu das Interface *org.jdesktop.application.Application.ExitListener* und registriert sich selbst mit *addExitListener()*. Die Methode *canExit()* entscheidet darüber, ob Versuche, die Anwendung zu beenden, erfolgreich sind (in diesem Fall liefert sie *true*) oder ob sie die Versuche einstellt. Wenn kein *ExitListener* sein Veto gegen das Beenden des Programms eingelegt hat, werden diese Interfaces in einem zweiten Schritt erneut benachrichtigt. Diesmal erfolgt ein Aufruf der Methode *willExit()*, die bei Bedarf allgemeine Aufräumarbeiten erledigt.

Anschließend ruft das Framework die beiden Methoden *shutdown()* und *end()* auf. Auch *shutdown()* kann gegebenenfalls Ressourcen freigeben. *end()* terminiert das Programm. Die Klasse *Application* nutzt hierzu *Runtime.getRuntime().exit(0)*. Neben den bereits vorgestellten Methoden können bei Bedarf weitere überschrieben werden. Informationen hierzu enthält die Dokumentation der Klasse *Application*.

Definierte Einsprungspunkte beim Starten und Beenden einer Anwendung helfen zweifellos, sie zu strukturieren. Und sie machen den Quelltext leichter lesbar. Das Öffnen eines Anwendungsfensters erfordert in den beiden Beispielen allerdings weiterhin eine Menge Infrastrukturcode.

Diesen macht die von *org.jdesktop.application.Application* abgeleitete Klasse *SingleFrameApplication* weitgehend überflüssig. Diese sowie die meisten anderen im Rahmen dieses Artikels vorgestellten Mechanismen demonstriert das in der Abbildung 2 gezeigte Programm *MiniChart*. (Dessen Quellcode ist über den *iX*-Listingservice erhältlich.)

Anlegen und Öffnen eines Fensters reduzieren sich auf den Aufruf der Methode *show()*. Als einzigen Parameter erwartet sie eine Komponente, die dessen Inhaltsbereich repräsentiert. Es bietet sich an, ihn in einer eigenen Methode zusammenzubauen und das Ergebnis an *show()* weiterzureichen. In *MiniChart.java* ist dies *buildMainView()*. Die für viele Anwendungen obligatorischen Elemente Menüleiste, Toolbar und Statuszeile zählen übrigens nicht zum Inhaltsbereich. Sie lassen sich bequem über eine automatisch erzeugte Instanz der Klasse *org.jdesktop.application.FrameView* setzen, die die Methode *getMainView()* liefert (Listing 3). Wie dies funktioniert, zeigt die Methode *buildMenubar()*.

## Eigenschaften in Dateien auslagern

Die Eigenschaften von Swing-Komponenten legen Aufrufe von „setXYZ()" fest. Dies ist in der Methode *startup()* der Klasse *Demo2* noch einigermaßen überschaubar, kann bei komplexeren Oberflächen allerdings schnell unleserlich und unübersichtlich werden. Aus diesem Grund sieht das Swing Application Framework vor, beliebige Komponenten-Eigenschaften in separate Dateien auszulagern.

Hierbei handelt es sich um gewöhnliche *.properties*-Dateien, die in Unterpaketen mit dem Namen *resources* liegen sollten. Zur Laufzeit liest das Frame-

work sie ein und „injiziert“ den zugehörigen Komponenten die darin enthaltenen Eigenschaften. Die Zuordnung erfolgt über einen beliebigen, aber eindeutigen Schlüssel, den die Komponenten-Methode *setName()* festlegt. Wie dies funktioniert, zeigt die Methode *buildMenubar()* der Klasse *MiniChart*. Die Eigenschaften enthält die Datei *MiniChart.properties* im Paket *com.thomaskuenneth.minichart.resources*. Hier ein Auszug:

```
# Menüleiste
menuFile.text = Datei
menuEdit.text = Bearbeiten
```

Properties sind Schlüssel-Wert-Paare. Der Schlüssel setzt sich aus zwei mit einem Punkt verbundenen Teilen zusammen: dem Namen der Komponente sowie der zu setzenden Eigenschaft. Eine Ausnahme von dieser Regel bilden sogenannte Aktionen, die im weiteren Verlauf des Artikels besprochen werden.

## Die Trennung von Daten und Code

Sofern es sich bei dem Wert nicht um einen String handelt, wird eine typspezifische Ersatzdarstellung verwendet. Beispielsweise bestimmen sich Vorder- und Hintergrundfarbe eines Labels durch Instanzen der Klasse *java.awt.Color*. Das Framework erwartet Farben entweder als sechsstellige Hexadezimalzahl mit einem vorangestellten # oder als eine Folge von drei durch ein Komma getrennten positiven ganzen Zahlen. Neben der Trennung von Daten und Code bietet das Auslagern von Komponenten-Eigenschaften als weiteren Vorteil eine leichte Lokalisierbarkeit. *.properties*-Dateien können für praktisch beliebig viele Sprachen vorgehalten werden.

Das Injizieren der Eigenschaften geschieht für die an *show()* übergebene Komponente und deren Kinder automatisch. Das Framework verwendet hierzu die Methode *injectComponents()* der Klasse *org.jdesktop.application.ResourceMap*. Der Programmierer kann sie für beliebige weitere Komponenten jederzeit von Hand aufrufen. Dies gilt auch für die Methode *injectFields()*. Sie befüllt allerdings stattdessen Instanzvariablen beliebiger Klassen. Wie dies funktioniert, zeigt Listing 4.

Zur Kennzeichnung von Instanzvariablen, denen Werte injiziert werden sollen, dient die Annotation *@Resource*. Die für den Start von Listing 4 notwendige *.properties*-Datei hat folgenden Inhalt:

```
Demo3.strText = Hallo Demo3
```

Der Schlüssel ergibt sich normalerweise aus den mit einem Punkt verbundenen Klassen- und Variablennamen, kann mit dem Konstrukt *(key="abc")* bei Bedarf aber überschrieben werden.

Bestimmte Benutzeraktionen, beispielsweise das Anklicken von Schaltflächen, melden in Swing *ActionEvents*. Durch das Registrieren von Listener und das Implementieren der nötigen *actionPerformed()*-Methoden kann viel Infrastrukturcode entstehen, der die Anwendung aufbläht und unleserlich macht. Hinzu kommt, dass unterschiedliche Komponenten oft die gleichen Aktionen auslösen sollen. Dies ist dann der Fall, wenn es zu einem Menüelement ein Pendant in der Toolbar gibt.

Deshalb bot es sich in solchen Situationen bisher an, das Interface *javax.swing.Action* zu implementieren oder von der Klasse *javax.swing.AbstractAction* abzuleiten, um Aktionen zu kapseln. Mit dem Swing Application Framework ist dies nicht mehr erforderlich. Die Annotation *@Action* kennzeichnet Methoden, die beim Feuern eines *ActionEvent* aufgerufen werden. Ein Aufruf der jeweiligen *setAction()*-Methode verbindet sie mit einer Komponente. Der Ausdruck *getContext().getActionMap().get()* ermittelt für einen Methodennamen die zugehörige Action. Er ist in *MiniChart.java* in der Methode *getAction()* gekapselt. Deren Einsatz zeigt die Methode *buildMenubar()* derselben Klasse.

Actions haben als Properties nicht nur einen Namen beziehungsweise einen anzuzeigenden Text, sondern können zusätzlich zwei Beschreibungen sowie ein Bild enthalten. Diese Elemente lassen sich zum einen über die Methode *putValue()* belegen und zum anderen – analog zu den Eigenschaften von Komponenten – in Properties-Dateien. Hier ein Auszug aus der Datei *MiniChart.properties*:

```
# Aktionen
quit.Action.text = Beenden...
quit.Action.shortDescription = ↵
                                    Beendet das Programm
quit.Action.icon = exit.png
```

Das Framework bietet darüber hinaus weitere Funktionen im Zusammenhang mit Actions, die allerdings einen eigenen Artikel wert sind. Als Anregung für eigene Experimente sei auf die be-

**Listing 2**

```
package com.thomaskuenneth.appframework;
import java.awt.BorderLayout;
import java.awt.Color;
import java.awt.Font;
import java.awt.event.WindowAdapter;
import java.awt.event.WindowEvent;
import java.util.EventObject;
import javax.swing.JFrame;
import javax.swing.JLabel;
import javax.swing.JOptionPane;
import org.jdesktop.application.Application;
import org.jdesktop.application.Application.ExitListener;

public class Demo2 extends Application implements ExitListener {
    private JFrame f = null;
    public static void main(String[] args) {
        Application.launch(Demo2.class, args);
    }
    @Override
    protected void startup() {
        addExitListener(this);
        f = new JFrame(getClass().getName());
        JLabel label = new JLabel("Hallo iX");
        label.setOpaque(true);
        label.setForeground(Color.green);
        label.setBackground(Color.black);
        label.setFont(Font.decode("Courier-72"));
        f.add(label, BorderLayout.CENTER);
        f.setDefaultCloseOperation(JFrame.DO_NOTHING_ON_CLOSE);
        f.addWindowListener(new WindowAdapter() {
            @Override
            public void windowClosing(WindowEvent e) {
                exit(e);
            }
        });
        f.pack();
        f.setLocationRelativeTo(null);
        f.setVisible(true);
    }
    @Override
    protected void shutdown() {
        f.setVisible(false);
        System.out.println("shutdown");
    }
    public boolean canExit(EventObject event) {
        if (JOptionPane.showConfirmDialog(f, "Anwendung beenden?")
                        == JOptionPane.YES_OPTION) {
            return true;
        }
        return false;
    }
    public void willExit(EventObject event) {
        System.out.println("Anwendung wird beendet");
    }
}
```

**Bevor die Methode *exit()* eine Anwendung beendet, benachrichtigt sie die registrierten *ExitListener*, die gegebenenfalls das Programmende verhindern.**

reits eingebaute Unterstützung des System-Klemmbretts durch drei vordefinierte Aktionen hingewiesen.

## Nebenläufigkeit verhindert Einfrieren

Auf die Eigenschaft von Swing, dass alle Änderungen an der Benutzeroberfläche (etwa das Setzen der Hintergrundfarbe) in einem bestimmten Thread abgewickelt werden müssen, hat dieser Artikel schon zu Beginn hingewiesen. Ein zwar naiver, allerdings leider recht verbreiteter Umgang mit dieser Vorgabe ist, sie zu ignorieren und einfach die gesamte Anwendung in diesem sogenannten Event Dispatching Thread ablaufen zu lassen. Allerdings findet in dessen Kontext auch das Zeichnen der Komponenten statt. Wenn ein

**Listing 3**

```
// Auszug aus der Klasse MiniChart
private void buildMenubar() {
        // das Datei-Menü
        menuFile = new JMenu();
        menuFile.setName("menuFile");
        menuFile.add(new JMenuItem(getAction("quit")));
        // das Bearbeiten-Menü
        menuEdit = new JMenu();
        menuEdit.setName("menuEdit");
        menuEdit.add(new JMenuItem(getAction("render")));
        // die Menüleiste bauen
        menuBar = new JMenuBar();
        menuBar.add(menuFile);
        menuBar.add(menuEdit);
        getMainView().setMenuBar(menuBar);
    }
private JComponent buildMainView() {
        JPanel p = new JPanel(new BorderLayout());
        textareaInput = new JTextArea();
        textareaInput.setName("textareaInput");
        JScrollPane scrollpaneInput = new JScrollPane(textareaInput);
        p.add(scrollpaneInput, BorderLayout.WEST);
        labelChart = new JLabel();
        labelChart.setName("labelChart");
        labelChart.setHorizontalAlignment(JLabel.CENTER);
        labelChart.setVerticalAlignment(JLabel.CENTER);
        labelChart.setPreferredSize(new Dimension(400, 300));
        p.add(new JScrollPane(labelChart), BorderLayout.CENTER);
        return p;
    }
```

***buildMainView* erzeugt den Inhalt des Fensters, für die Menüleiste sorgt *buildMenubar*.**

**Listing 4**

```
package com.thomaskuenneth.appframework;
import javax.swing.JLabel;
import org.jdesktop.application.Resource;
import org.jdesktop.application.SingleFrameApplication;

public class Demo3 extends SingleFrameApplication {
    @Resource
    String strText;
    public static void main(String[] args) {
        launch(Demo3.class, args);
    }
    @Override
    protected void startup() {
        getContext().getResourceMap().injectFields(this);
        show(new JLabel(strText));
    }
}
```

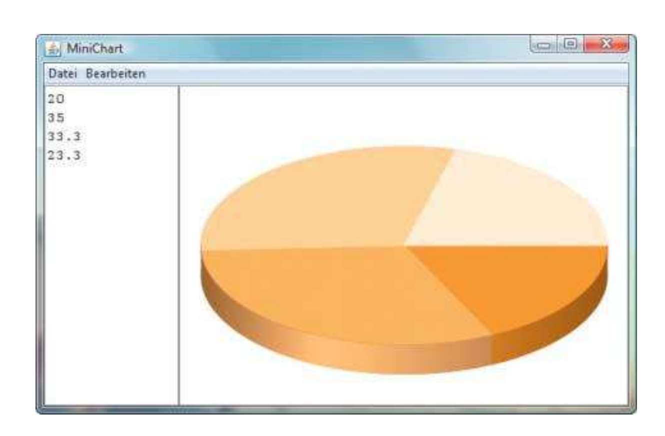
**Mit *injectFields()* kann man die Werte von Instanzvariablen beliebiger Klassen setzen.**

**Listing 5**

```
// Auszug aus der Klasse MiniChart
    @Action
    public Task render() {
        return new Task<Image, Void>(Application.getInstance()) {
            @Override
            protected Image doInBackground() {
                float[] data = GoogleChart.parseString(
                                        textarea Input.getText());
                String url = GoogleChart.createPieChart(true,
                                                400, 300, data);
                System.out.println(url);
                return GoogleChart.getChartAsImage(url);
            }
            @Override
            protected void succeeded(Image result) {
                labelChart.setIcon(new ImageIcon(result));
            }
        };
    }
```

**Eine mit *@Action* annotierte Methode läuft in einem eigenen Thread.**

**Die Methode *show()* legt ein Fenster an und öffnet es. Ihr einziger Parameter bestimmt dessen Inhalt (Abb. 2).**




Programm komplexe Berechnungen ausführt oder auf Ergebnisse eines Serverzugriffs wartet, führt dies konsequenterweise zu einem „Einfrieren“ der Oberfläche. Nicht zuletzt aus diesem Grund haben Swing-Anwendungen den Ruf, langsam und träge zu sein.

Der Programmierer muss also dafür sorgen, dass seine Anwendung „Langläufer“ in einem separaten Hintergrund-Thread abarbeitet. Sun unterstützt ihn hierbei mit der Klasse *javax.swing.SwingWorker*, die seit Java SE 6.0 zum Standard gehört. Änderungen von Komponenteneigenschaften hingegen gehören in die Obhut des EDT. Hierfür stehen schon seit geraumer Zeit die Methoden *invokeAndWait()* und *invokeLater()* der Klasse *javax.swing.SwingUtilities* zur Verfügung.

Das Swing Application Framework greift das *SwingWorker*-Konzept auf und erweitert es zu sogenannten Tasks. Diese lassen sich auf bequeme Weise mit Aktionen verknüpfen. Liefert eine mit *@Action* annotierte Methode eine Instanz der Klasse *org.jdesktop.application.Task*, läuft diese beim Auslösen der Aktion in einem eigenen Thread. Wie eine solche Implementierung aussehen kann, zeigt die Methode *render()* der Klasse *MiniChart* (Listing 5).

Auch Tasks durchlaufen also einen Lebenszyklus, der sich in verschiedenen Methoden manifestiert. Die beiden wichtigsten Stationen in diesem Beispiel sind *doInBackground()* sowie *succeeded()*. Letztere ist dafür gedacht, nach dem erfolgreichen Abschluss einer nebenläufigen Aktivität die Oberfläche zu aktualisieren. Die Methoden *cancelled()*, *interrupted()* und *failed()*, deren Ausführung im EDT erfolgt, erlauben einer Anwendung, auf Fehler oder einen vorzeitigen Programmabbruch zu reagieren.

*Task* beziehungsweise *SwingWorker* sehen übrigens auch Mechanismen vor, mit denen sich während der Abarbeitung Komponenteneigenschaften verändern lassen. Beispielsweise kann die Anwendung die Methode *process()* überschreiben und bei Bedarf *publish()* aufrufen. Die beiden Klassen *TaskMonitor* und *TaskService* ermöglichen die Kontrolle von Hintergrundaktionen und stellen zusätzliche Mechanismen für die Ausgabe von Statusinformationen zur Verfügung. Auf sie kann der Artikel aus Platzgründen allerdings nicht weiter eingehen.

## Session-Management leicht gemacht

Es gehört zum guten Ton, den Zustand einer Anwendung beim Beenden zu sichern und bei einem erneuten Programmstart wiederherzustellen. Üblicherweise speichert man die Position und Größe ihrer Fenster sowie die wichtiger Oberflächenelemente. Bisher musste der Swing-Programmierer diese Aufgabe komplett selbst übernehmen, also alle relevanten Werte abfragen, mithilfe der Klasse *java.util.prefs.Preferences* speichern und später wieder auslesen. Das Swing Application Framework übernimmt einen großen Teil dieser Arbeit, sofern die Anwendung von der Klasse *SingleFrameApplication* ableitet. In dem Fall legt die Klasse *Session-*

**Listing 6**

```
@Override protected void startup() {
    ApplicationContext appContext = getContext();
    appContext.setVendorId("Heise");
    appContext.setApplicationId("iX-Demo");
    // Benutzeroberfläche bauen
    appContext.getSessionStorage().restore(mainFrame,
                                "session.xml");
}
```

**Aus *session.xml* liest die Anwendung bei einem erneuten Start den letzten Zustand der Fenster und einiger Komponentenarten.**

*Storage* den Zustand der Fenster sowie einiger weiterer Komponentenarten (*JTable, JSplitPane* und *JTabbedPane*) automatisch in einer XML-Datei ab beziehungsweise liest diese Informationen wieder aus ihr.

Mithilfe der Klasse *ApplicationContext* kann man auf eine Instanz von *SessionStorage* zugreifen. Das folgende Quelltextfragment schreibt die Datei *session.xml*:

```
@Override protected void shutdown() {
    getContext().getSessionStorage().save ↵
                    (mainFrame, "session.xml");
}
```

Listing 6 demonstriert das Einlesen. Der Speicherort der Datei ist plattformabhängig. Unter Windows Vista befindet er sich beispielsweise im Unterverzeichnis *AppData\Roaming* des Heimatverzeichnisses des angemeldeten Benutzers.

## Fazit

Dieser Artikel konnte natürlich nicht alle Aspekte des Swing Application Framework umfassend beleuchten. Er macht aber deutlich, dass es seinem Anspruch, das Erstellen von Swing-Anwendungen stark zu vereinfachen, gerecht wird. Das Framework entlastet Entwickler von unnötiger Schreibarbeit und hilft ihm dabei, die Anwendung besser zu strukturieren. Dies betrifft nicht nur den Lebenszyklus des Programms, sondern auch das Auslagern von Komponenteneigenschaften in Properties-Dateien. Gerade für Einsteiger sind das Übernehmen von Routineaufgaben wie das Sichern und Wiederherstellen von Sitzungen sowie das elegante Verdrahten von Actions mit Methoden sicherlich eine willkommene Entlastung.

Natürlich gibt es in Swing eine Reihe weiterer Baustellen, die ein Anwendungs-Framework abdecken könnte. Als Beispiel sei hier nur auf das Binden von Komponenten an Attribute eines Domänenmodells verwiesen. Dieser Problematik widmet sich ebenfalls ein Java Specification Request: JSR-295 (Beans Binding).

Wie elegant die beiden Puzzleteile letztlich zusammenpassen, kann erst ein Blick auf die endgültige Version von Java 7 zeigen. Bis dahin wird sich wahrscheinlich auch die eine oder andere Funktionsweise des Swing Application Framework noch ändern. So werden dessen Klassen sicherlich in einem Unterpaket von *javax.swing* liegen. Dies sollte man bei einer Verwendung des Prototyps unbedingt berücksichtigen. (ka)

**Onlinequellen**

SR 296: Swing Application Framework http://jcp.org/en/jsr/detail?id=296

Prototyp des Swing Application Framework https://appframework.dev.java.net/

THOMAS KÜNNETH

arbeitet als Spezialist für Client-Technologien im Team Anwendungsarchitektur einer großen Bundesbehörde. Neben zahlreichen Artikeln hat er zwei Bücher über Java und Eclipse veröffentlicht.









Bacula steuert Bandbibliotheken

# Regisseur

**Daniel Wedewardt**

Ein Backup-System, das professionellen Ansprüchen genügt, muss nicht teuer sein. Allerdings sollte der Administrator zum Einrichten ein wenig Zeit mitbringen. *iX* hat es mit Debian, Bacula und einer Bandbibliothek durchexerziert.

Unternehmen kommen nicht darum herum, ihre Backup-Strategie regelmäßig zu überprüfen – und, falls nötig, zu ändern. Beim Autor stellte sich die Frage, ob die bisher durchgeführte reine Festplattensicherung den Anforderungen noch genügt. Angesichts der Menge von mehreren Terabyte aktiver Daten, dem Bedürfnis nach längeren Vorhaltezeiten und einem verhältnismäßig kleinen Budget fiel die Entscheidung für einen Wechsel auf die in der Anschaffung zwar teurere, aber im Betrieb deutlich günstigere LTO-4-Bandtechnik mit Tape-Robotik, konkret auf eine Tandberg Storagelibrary T40 mit zwei Laufwerken, FC-Anschluss, 24 Slots (ausbaubar auf 32) und Barcode-Reader.

## Erste Hürde Fibre Channel

Als Backup-Software sollte weiterhin Bacula (www.bacula.org) zum Einsatz kommen [1]. Zwar verspricht die Dokumentation der Open-Source-Software generell Unterstützung für Autoloader, das Modell Tandberg T40 stand jedoch nicht auf der Liste der getesteten Geräte. Selbst Tandberg war nicht in der Lage, eine Machbarkeitsgarantie auszustellen, schon gar nicht unter Debian Linux. Es blieb daher nur, Klarheit zu schaffen und eine Testphase zu vereinbaren.

Die Storagelibrary verfügt über zwei FC-Ports und eine Ethernet-Schnittstelle. Letztere dient als Management-Interface und hat im täglichen Betrieb keine Bedeutung. Da im Unternehmen noch kein SAN vorhanden war, sollte die Library direkt mit einem FC-HBA von Qlogic im Backup-Server kommunizieren.

Allerdings besitzt Debian dafür standardmäßig keine Treiber, und Qlogic unterstützt offiziell nur die beiden Enterprise-Distributionen RHEL und SLES. Bindet man jedoch den *non-free*-Zweig in */etc/apt/sources.list* als Installationsquelle ein, kann man mit *apt-get install firmware-qlogic* die benötigten Dateien nachinstallieren.

Funktioniert der Treiber, tauchen in */dev* die neuen Geräte auf. Die Bandlaufwerke sogar mehrfach: *st<nummer>* und *nst<nummer>* dienen dem Datentransfer; das zugehörige „Generic SCSI Device“ *sg<nummer>* erlaubt den direkten Zugriff, kommt aber beim Backup nicht zum Einsatz. Die Robotik hingegen ist ausschließlich über ein Generic Device zugänglich. Hinter welchem Device sich welches Gerät verbirgt, verrät der Befehl *sg_map –i –x* (siehe Listing 1). Detailinformationen zu den einzelnen Geräten liefert *tapeinfo –f /dev/sg<nummer>*.

Bereits ohne Backup-Software sind die ersten rudimentären Tests möglich. Mit dem Kommando */usr/sbin/mtx –f /dev/sg<nummer> load 1 0* etwa kann man die Robotik anweisen, das Band aus Slot 1 ins erste Laufwerk zu transportieren. Schreib- und Lesetests lassen sich zum Beispiel mit *tar* durchführen.

Leider haben das Betriebssystem und die Robotik – der sogenannte „Changer“ – unterschiedliche Auffassungen darüber, wie die Laufwerke zu nummerieren sind. Es ist daher ratsam, die Bandlaufwerke bei der Installation zunächst in derselben Reihenfolge anzuschließen, wie sie der Changer verwaltet. Später kann man *udevd* anweisen, feste Namen für die Geräte zu vergeben [2]. Auch „sprechende“ Gerätenamen lassen sich einrichten, etwa */dev/library/drive<nummer>* und */dev/library/changer* für Laufwerke beziehungsweise Robotik.

Anschließend gilt es, Backup-Software und Tape-Library miteinander bekannt zu machen. Es ist ratsam, in */etc/bacula/bacula.sd.conf* zunächst den Storage Daemon einzurichten. Listing 2 zeigt die zusätzlichen Einträge für den Changer und das erste Bandlaufwerk.

Über den selbst gewählten Namen *StorageLibraryT40* des Autochangers kann man anschließend in der Director-Konfigurationsdatei *bacula-dir.conf* auf die Bandbibliothek verweisen (siehe Listing 3). Wie man im Konfigurationsobjekt *Storage* sieht, muss der Storage Daemon nicht auf demselben Server laufen wie der Director.

Das Attribut *Cleaning Prefix = CLN* im Konfigurationsobjekt *Pool* bewirkt, dass Bacula Bänder, deren Barcode mit *CLN* beginnt – dem Standardkürzel für Reinigungsbänder –, nicht in den Pool aufnimmt. So verhindert man, dass Bacula versehentlich ein Reinigungsband als Sicherungsmedium verwendet.

Von Zeit zu Zeit muss der Administrator die Tape Library mit neuen Bändern füttern. Nach dem Einlegen neuer Bänder liest die Storagelibrary automatisch deren Barcode-Aufkleber. Gibt der Administrator in der Bacula-Konsole *bconsole* den Befehl *label barcodes* ein, schreibt die Backup-Software zusätzlich ein Label aufs Band. Das vermeidet Verwechselungen und stellt obendrein sicher, dass sich die Bänder auch ohne Barcode-Reader noch zuordnen lassen.

Ebenso einfach lässt sich ein Magazinwechsel durchführen. Das *bconsole*-Kommando *unmount* weist die Bandbibliothek an, alle Bänder aus den

Laufwerken zu werfen und in ihre jeweiligen Slots zurückzubefördern. Anschließend kann der Operator ein oder mehrere Magazine austauschen und schließlich mit *update slots* die Statusinformationen der Library neu einlesen.

## Fazit

Zwar ist Bacula nicht so komfortabel wie manche kommerzielle Lösung, es bietet jedoch einen vergleichbaren Funktionsumfang bei erheblich geringeren Kosten. Die Kombination aus Bacula und Bandbibliothek ist nach dem erfolgreichen Abschluss der Testphase mittlerweile im produktiven Einsatz und hat dem Backup-Administrator die Arbeit erheblich erleichtert: Abgesehen von gelegentlichen Magazinwechseln und den obligatorischen regelmäßigen Probe-Wiederherstellungen kann er das System sich selbst überlassen. (mr)

DANIEL WEDEWARDT

ist IT-Manager bei der Native Instruments GmbH in Berlin.

**Listing 1: *sg_map* zeigt die Zuordnung der Geräte**

```
/dev/sg0  0 0 2 0  0  /dev/sda  easyRAID   S8A2           R0.0
/dev/sg1  1 0 1 0  0  /dev/sdb  easyRAID   S8A2           R0.0
/dev/sg2  2 0 0 0  1  /dev/nst0  IBM       ULTRIUM-TD4     74H4
/dev/sg3  2 0 0 1  8  TANDBERG  StorageLoader    0317
/dev/sg4  3 0 0 0  1  /dev/nst1  IBM       ULTRIUM-TD4     74H4
```

**Listing 2: Konfiguration des Storage-Daemons**

```
Autochanger {
  Name = StorageLibraryT40
  Device = Drive-0, Drive-1
  Changer Command = "/etc/bacula/scripts/mtx-changer %c %o %S %a %d"
  Changer Device = /dev/sg3
}
Device {
  Name = Drive-0
  Drive Index = 0
  Device Type = Tape
  Media Type = Tape
  Archive Device = /dev/nst0
  AutomaticMount = yes;
  AlwaysOpen = yes;
  RemovableMedia = yes;
  RandomAccess = no;
  AutoChanger = yes
  # Enable the Alert command only if you have the mtx package loaded
  #Alert Command = "sh -c 'tapeinfo -f %c |grep TapeAlert|cat'"
  Spool Directory = /mnt/backup0/bacula/spool
}
```

**Listing 3: Auszug aus der Director-Konfiguration**

```
JobDefs {
  Name = "DefaultJob"
  Type = Backup
  Level = Full
  Client = backup-fd
  FileSet = "Full Set"
  Schedule = "WeeklyCycle"
  Storage = StorageLibraryT40
  Messages = Standard
  Pool = Tapes
  Priority = 10
  SpoolData = yes
  Prefer Mounted Volumes = no
}
Storage {
  Name = StorageLibraryT40
  Address = 192.0.2.40
  SDPort = 9103
  Password = "<PASSWORT>"
  Device = StorageLibraryT40
  Media Type = Tape
  Maximum Concurrent Jobs = 5
  Autochanger = yes
}
Pool {
  Name = Tapes
  Pool Type = Backup
  AutoPrune = yes
  Volume Retention = 1d
  Maximum Volumes = 19
  Recycle = yes
  Recycle Oldest Volume = yes
  Cleaning Prefix = "CLN"
}
```

### Literatur

[1] Jan-Piet Mens; Datensicherung; Rückversicherung; Open-Source-Backup-Software im Vergleich; *iX* 9/2007, S. 48

[2] Michael Riepe; Linux-Systemverwaltung; Gerätemacher; Wie der Linux-Daemon *udevd* funktioniert; *iX* 7/2007, S. 131

**iX-Link ix0807136**








Bilddateien in Java-Anwendungen nutzen

# Zeigt her eure Bildchen

**Jürgen Key**

Von Haus aus unterstützt Java nur relativ wenige Bildformate. Weitere lassen sich mithilfe des *ImageIO*-Framework laden. Eine kleine Anwendung zeigt, wie sich ein neuer *ImageReader* implementieren lässt.

Beim Laden und Benutzen von Bilddateien in Java-Programmen gibt es einige Hürden zu überwinden. Die diversen Wege, die ans Ziel führen, unterscheiden sich durch subtile Kleinigkeiten. Gleichgültig, welche Methode man letztlich einsetzt – keine versteht von Haus aus besonders viele Bildformate.

Java unterstützt (ohne zwischen den einzelnen Methoden zu differenzieren) zunächst JPEG und GIF. Mit Version 1.4 kamen PNG und (W)BMP hinzu. Dieser etwas kümmerliche Satz von unterstützten Formaten lässt sich jedoch bei Bedarf einfach und elegant erweitern. Das Schöne daran: Man braucht bestehende Anwendungen nicht zu ändern, da die neuen Formate nicht in eine bestimmte Anwendung, sondern in die Laufzeitumgebung integriert werden. Danach können alle Anwendungen von den neuen Möglichkeiten profitieren.

Natürlich könnte man die Bilder einfach in eines der genannten Formate konvertieren. Das bedeutet aber, dass man zunächst passende Konverter finden muss. Diese dann auf die gesammelten Schätze aus frühen Raytracing-Tagen oder auf die letzte Lieferung von CRT-Bildern loszulassen, bedeutet im schlimmsten Fall Handarbeit und eine Menge Bedenkzeit seitens des Rechners. In manchen Einsatzszenarien schließt sich Konvertieren sogar ganz aus – etwa bei der Archivierung von Aufnahmen. Dabei kommt es auf den Erhalt des Originalzustands an, zu dem eben auch das ursprüngliche Format gehört.

## Urgestein *Toolkit* hat enge Grenzen

Die Klasse *Toolkit* existiert im Namensraum *java.awt* schon fast so lange wie es Java gibt – nämlich seit dem JDK 1.0. Sie bietet zwei Alternativen zum Laden eines Bildes an: *getImage* und *createImage*.

Die Methode *createImage* existiert gleich in fünf Varianten. Am wichtigsten für das Laden von Bildern sind die zwei, die einen String beziehungsweise eine URL als Speicherort einer Bilddatei übergeben bekommen. Diese Varianten gibt es für die Methode *getImage* ebenfalls. Der Unterschied zwischen beiden ist, dass *getImage* intern Referenzen auf geladene Bilder hält. Fordert eine Anwendung dasselbe Bild mehrfach an, liefert *getImage* einfach eine Referenz auf die geladenen Daten zurück. Die Vorteile liegen auf der Hand: Der Speicherverbrauch verringert sich, und wiederholte Zugriffe auf dasselbe Bild laufen schneller ab.

Allerdings kann die Klasse *Toolkit* nicht entscheiden, wann die gepufferten Bilddaten nicht mehr benötigt werden. Eine Anwendung muss nicht mehr benötigte Bilddaten explizit beseitigen. Diesen Nachteil hat *createImage* nicht, da die Methode intern keine Referenzen hält. Bei ihrem Einsatz lädt eine Anwendung dasselbe Bild unter Umständen mehrfach, dafür werden nicht mehr referenzierte Bilddaten jedoch automatisch Opfer des Garbage Collector.

Der größte Nachteil, den beide Methoden aufweisen, ist der, dass sie nicht

**iX-TRACT**

- Java unterstützt von Haus aus nur die Bildformate JPEG und GIF, mit der Version 1.4 sind PNG und (W)BMP hinzugekommen.
- Nicht in allen Fällen will man Bilder in andere Formate konvertieren, um sie in Java-Programme laden zu können.
- Abhilfe kann das *ImageIO*-Framework schaffen, mit dem Entwickler zusätzliche *ImageReader* implementieren können.

einmal mit allen eingangs genannten Bildformaten umgehen können: Die Unterstützung für (W)BMP fehlt. Zudem lässt sich die Klasse *Toolkit* nicht dahin gehend erweitern, dass sie weitere Formate unterstützt.

## Laden der Bilddateien erfolgt asynchron

Weiterer potenzieller Nachteil: Die Methoden arbeiten asynchron. Das bedeutet, dass nach der Rückkehr aus dem Aufruf einer solchen Methode das Bild noch lange nicht geladen ist. Um zu erkennen, wann eine Anwendung tatsächlich Zugriff auf die Bilddaten hat, kann man sich eines sogenannten *MediaTracker*-Objekts bedienen. Daraus folgte in der Praxis der umständliche Einsatz von *MediaTracker*-Code überall dort, wo Bilder geladen werden, nur um den asynchronen Ansatz auszuhebeln und das Laden eines Bildes synchron zu erledigen.

Ein Beispiel dafür findet man in der Klasse *examples.ViewerOld*, die dieses Vorgehen nutzt, um gefahrlos Breite und Höhe des geladenen Bildes zu ermitteln. Die genannte Klasse ist Teil des Beispielcodes zu diesem Artikel, der über den *iX*-Listingserver erhältlich ist. Der Code der Klassen *Viewer* und *ViewerOld* wurde aus dem im Web verfügbaren *Viewer.java* abgeleitet (siehe „Onlinequellen“ [a]).

Besser geht es mit *ImageIO*. Seit Java 1.4 existiert der neue Namensraum *javax.imageio*. Wie die Bezeichnung vermuten lässt, handelt es sich bei den Klassen unterhalb dieses Namensraums um solche zum Laden und Speichern von Bildern. Die mit Java gelieferte Implementierung unterstützt die Formate, mit denen auch die Klasse *java.awt.Toolkit* klarkommt. Darüber hinaus kann *ImageIO* BMP- und WBMP-Dateien lesen und schreiben. GIF-Dateien kann man nur lesen, eine Speicherung ist in Java-Anwendungen ohne zusätzliche Hilfsmittel nicht möglich.

Das Laden und Speichern von Bildern erfolgt synchron – man kann die Operationen aber bei Bedarf in Threads auslagern. Die zentrale Schnittstelle zum *ImageIO*-Subsystem ist die Klasse *javax.image.ImageIO*. Sie verfügt über mehrere *read*-Methoden zum Laden von Bildern, die unterschiedliche Parametertypen haben, die den Ort bezeichnen, an dem die Methode ein Bild findet. Jede dieser Methoden erzeugt eine Instanz der Klasse *BufferedImage* aus dem Namensraum *java.awt.image*, die von *Image* in *java.awt* abgeleitet ist. Dadurch lässt sich alter, auf *Toolkit* aufbauender Code elegant durch *ImageIO* ersetzen.

Die Methoden zum Speichern von Bildern erwarten die Bilddaten in einer Implementierung des Interface *RenderedImage* aus dem Namensraum *java.awt.image*. Dieses Interface implementiert beispielsweise die Klasse *Buffered Image* – so schließt sich der Kreis zwischen Laden und Speichern auf elegante Weise.

Zurück zur transparenten Erweiterung einer Java-Implementierung um die Unterstützung für weitere Bildformate. Der Namensraum *javax.imageio* ist konsequent darauf ausgerichtet, weitere Formate sowohl beim Speichern als auch beim Laden zu erlauben. Eine Unterstützung neuer Formate erreicht man durch die Erweiterung des Klassenpfads um neue *ServiceProvider*. Das kann einesteils explizit geschehen, andererseits – und das ist der Clou – durch das Kopieren einer entsprechenden JAR-Datei in das Verzeichnis, in dem die Extensions der jeweiligen Java-Laufzeitumgebung verwaltet werden (meistens das Unterverzeichnis *lib/ext* im Installationsverzeichnis der Laufzeitumgebung) (siehe [b] und [c]).

## *ServiceProvider* liefern Formate

Damit die VM die neuen *ServiceProvider* erkennt, muss in einem solchen Archiv eine Datei existieren, die die benötigten Informationen bereitstellt. Speicherort dieser Datei ist *META-*

**Listing 1: Auszug aus *TGAReaderSpi.java***

```
public TGAReaderSpi()
{
    super("NetSys.IT",
        "0.0.1",
        new java.lang.String[]{"tga","tpic"},
        new java.lang.String[]{".tga",".tpic"},
        new java.lang.String[]{"image/x-tga",
                               "image/x-targa"},
        "ix.imageio.tga.TGAReader",
        new java.lang.Class[]{
       javax.imageio.stream.ImageInputStream.class},
        null,
        false,
        null,
        null,
        null,
        null,
        true,
        null,
        null,
        null,
        null);
}

public boolean canDecodeInput(java.lang.Object source)
{
    boolean rv=false;
        if(source instanceof
                javax.imageio.stream.ImageInputStream)
        {
            javax.imageio.stream.ImageInputStream
              is=(javax.imageio.stream.ImageInputStream)
              source;
            is.mark();
            byte[] header=new byte[3];
            try{
            if(is.read(header)==3)
            {
                int tgatype=header[2];
                System.out.println("tgatype "+tgatype);
                //For illustration purposes: we do only
                //support a subset of possible
                //tga image types here!
                rv=(((tgatype==ix.imageio.tga.TGARea
der.TRUE_COLOR)||(tgatype==ix.imageio.tga.TGAReader.BLACK_A
ND_WHITE))||((tgatype==ix.imageio.tga.TGAReader.RLE_TRUE_CO
LOR)||(tgatype==ix.imageio.tga.TGAReader.RLE_BLACK_AND_WHI
TE)));
            }
            is.reset();
            }catch(java.io.IOException exp){}
        }
        return rv;
    }
```

**Nach der Überprüfung darauf, ob es sich um einen unterstützten TGA-Typ handelt, lädt die Klasse *ix.imageio.spi.TGAReaderSpi* gegebenenfalls die Bilddatei und gibt sie aus.**

**Parameter eines *ServiceProvider***

| Name | Wert |
|---|---|
| *vendorName* | Name des Autors |
| *version* | Versions-Identifier |
| *names* | Formatnamen (mindestens einer) |
| *suffixes* | Dateiendungen (mindestens eine) |
| *MIMETypes* | Strings, die die Mimetypes des betreffenden Formats darstellen (mindestens einer) |
| *readerClassName* | Name (voll qualifiziert mit Namensraum) der zugehörigen *ImageReader*-Klasse |
| *inputTypes* | Menge von Klassenobjekten, die als Input für die *ImageReader*-Klasse dienen können |

**Unterstützte TGA-Typen**

| Typ | Beschreibung | unterstützt |
|---|---|---|
| 0 | keine Bilddaten enthalten | nein |
| 1 | nicht komprimiert, farblich verändertes Bild (Color Mapping) | nein |
| 2 | nicht komprimiert, Echtfarbbild | ja |
| 3 | nicht komprimiert, Graustufenbild | ja |
| 9 | lauflängenkodiert, farblich verändertes Bild (Color Mapping) | nein |
| 10 | lauflängenkodiert, Echtfarbbild | ja |
| 11 | lauflängenkodiert, Graustufenbild | ja |

**Listing 2: Auszug aus *TGAReader.java***

```
public class TGAReader extends javax.imageio.ImageReader
{
     public static final int COLOR_MAPPED=1;
     public static final int TRUE_COLOR=2;
     public static final int BLACK_AND_WHITE=3;
     public static final int RLE_COLOR_MAPPED=9;
     public static final int RLE_TRUE_COLOR=10;
     public static final int RLE_BLACK_AND_WHITE=11;
     public static final int NO_TGA=0;
     private int height=-1;
     private int width=-1;
     private int depth=-1;
     private byte specs=-1;
     private int tgatype=NO_TGA;
     private int charmax=-1;
     private int colormaplength;
     private int colormapfirstindex;
     private int colormaplayout;
     private int idlength;

     public java.awt.image.BufferedImage read(
        int imageIndex, javax.imageio.ImageReadParam param)
     {
          java.awt.image.BufferedImage bi=null;
          java.lang.Object inputref=getInput();
          javax.imageio.stream.ImageInputStream
          is=(javax.imageio.stream.ImageInputStream)inputref;
          try
          {
               readHeader(is);
               readExtent(is);
               int pixelcount=width*height;
               byte[] buf=null;
               int byteperpixel=depth/8;
               if(depth%8!=0)
                    byteperpixel+=1;
//Hier exemplarisch nur eine moegliche Kodierung behandelt
               if (tgatype==
                   ix.imageio.tga.TGAReader.TRUE_COLOR)
               {
                    int rowbytes=width*byteperpixel;
                    buf=new byte[rowbytes];
                    if(depth>24)
                         bi=new java.awt.image.BufferedImage
(width,height,java.awt.image.BufferedImage.TYPE_INT_ARGB);
                    else
                         bi=new java.awt.image.BufferedImage
(width,height,java.awt.image.BufferedImage.TYPE_INT_RGB);
                    for (int y = 0; y < height; ++y)
                    {
                         is.read(buf);
                         int x=0;
                         int uy=y;
                         if((specs&0x20)==0)
                              uy=height-1-y;
                         while(x<width)
                         {
                              int color=0;
                              if(depth>24)
                                   color=convert(buf[3+x*byte
perpixel])*16777216+convert(buf[2+x*byteperpixel])*65536+con
vert(buf[1+x*byteperpixel])*256+convert(buf[0+x*byteperpi
xel]);
                              else
                                   color=convert(buf[2+x*byte
perpixel])*65536+convert(buf[1+x*byteperpixel])*256+convert
(buf[0+x*byteperpixel]);
                              int ux=x;
                              if((specs&0x10)!=0)
                                   ux=width-1-x;
                              bi.setRGB(ux,uy,color);
                              ++x;
                         }
                    }
               }
          }
          catch(java.io.IOException exp)
          {
               exp.printStackTrace();
          }
          return bi;
     }
     private void readImageSpecs()
     {
          java.lang.Object inputref=getInput();
          if(inputref instanceof
                    javax.imageio.stream.ImageInputStream)
          {
//Wichtig: Stream zuruecksetzen auf Anfang,
//nachdem der Header gelesen wurde!
               javax.imageio.stream.ImageInputStream is=(ja
vax.imageio.stream.ImageInputStream)inputref;
               is.mark();
               try{
                    readHeader(is);
               is.reset();
               }catch(java.io.IOException exp){}
          }
     }

     private void readHeader(javax.imageio.stream.ImageInput
Stream is)throws java.io.IOException
     {
          byte[] buf=new byte[10];
          boolean advance=true;
          //length of image id field
          advance=is.read(buf,0,1)==1;
          if(advance)
          {
               idlength=convert(buf[0]);
          }
          //image type
          if(advance)
               advance=is.read(buf,0,2)==2;
          if(advance)
          {
               tgatype=buf[1];
               //For illustration purposes: we do only
               //support a subset of possible
               //tga image types here!
if(((tgatype!=TRUE_COLOR)&&(tgatype!=BLACK_AND_WHITE))&&((tg
atype!=RLE_TRUE_COLOR)&&(tgatype!=RLE_BLACK_AND_WHITE)))
                    tgatype=NO_TGA;
          }
          //colormap specs
          if(advance)
               advance=is.read(buf,0,5)==5;
          if(advance)
          {
               colormaplength=convert(buf[3])
               *256+convert(buf[2]);
          }
          //image specs
          if(advance)
               advance=is.read(buf,0,10)==10;
          if(advance)
          {
               //origins here are omitted!
               //image width
               width=convert(buf[5])*256+convert(buf[4]);
               //image height
               height=convert(buf[7])*256+convert(buf[6]);
               //image depth
               depth=buf[8];
               //specs
               specs=buf[9];
          }
     }
}
```

**Die Klasse *TGAReader* implementiert das Interface *ImageReader*, um Bilder über *ImageIO* laden zu können.**

*INF/services*. Der Name der Datei entspricht dem des *ServiceProvider*, der durch die jeweilige Extension implementiert wird. Das könnte für das Laden und Speichern von Bildern zum Beispiel *javax.imageio.spi.ImageReaderWriterSpi* sein (der Dateiname ergibt sich durch den voll qualifizierten Namen der *ServiceProvider*).

Das Beispielprogramm kümmert sich lediglich um das Laden von Bildern – daher heißt die Datei hier *javax.imageio.spi.ImageReaderSpi*. Sie enthält den Namen der konkreten *ServiceProvider*-Implementierung – da das Beispiel Java zum Umgang mit TGA-Dateien (Targa Image Filename [d]) befähigen soll, also *ix.imageio.spi.TGAReaderSpi* (Listing 1). Diese Klasse enthält noch keinen Code, der sich tatsächlich mit der Analyse des TGA-Formats beschäftigt. Laut Kontrakt ist sie so zu schreiben, dass eine schnelle Instanziierung erfolgen kann. Vor allem sollte sie idealerweise keine Abhängigkeiten zu externen Klassen aufweisen.

Abgeleitet wird die Klasse von *javax.imageio.spi.ImageReaderSpi* und ruft logischerweise den Basisklassenkonstruktor auf. Beim Aufruf des Basisklassenkonstruktors werden nur Werte für die Parameter übergeben, die unumgänglich sind. Für die anderen Parameter übergibt man einfach Null. Tabelle 1 zeigt die Parameter und ihre Bedeutung.

## Wie immer: Je schneller, desto lieber

Die Klasse erfüllt drei Aufgaben: Sie soll Auskunft darüber geben, was genau sie leisten soll. Im Beispielprogramm liefert die Methode *getDescription* einfach den String „TGA“ zurück. Da diese Methode eine Locale übergeben bekommt, kann (und sollte) man hier aussagekräftige Formulierungen wählen, die jeder Benutzer des Programms versteht. Weiterhin bietet die Klasse eine Methode *canDecodeInput*, die über einen schnellen Check herausfindet, ob der übergebene Container Daten enthält, die die vorliegende Implementierung verarbeiten kann. Auch hier gilt wieder: Je schneller, desto besser. Das Beispielprogramm greift dabei auf Byte 3 der Daten zurück und prüft, ob es sich um einen unterstützten Typ eines TGA-Bildes handelt.

Als Drittes schließlich liefert die Methode *createReaderInstance* eine Implementierung des Interface *Image Reader* aus dem Namensraum *javax.imageio*. Ob sie eine entsprechende Instanz jedes Mal neu erzeugt oder die Anforderung durch Zugriff auf einen Pool wiederverwendbarer Instanzen bedient, ist dem jeweiligen Entwickler freigestellt. Das Beispiel stellt eine Implementierung dieses Interface namens *TGAReader* im Namensraum *ix.imageio.tga* zur Verfügung, die es bei jedem Aufruf der Methode *createReaderInstance* neu instanziiert.

Die eigentliche Implementierung des Parsers, der die Umsetzung der Rohdaten in eine Instanz der Klasse *Buffered-*

## Onlinequellen

| | |
|---|---|
| [a] *Viewer.java* | schmidt.devlib.org/java/load-image-toolkit.html |
| [b] Packaging Programs in JAR Files | java.sun.com/docs/books/tutorial/deployment/jar/ |
| [c] Understanding Extension Class Loading | java.sun.com/docs/books/tutorial/ext/basics/load.html |
| [d] TGA File Format | tfcduke.developpez.com/tutoriel/format/tga/fichiers/tga_specs.pdf |

*Image* übernimmt, steckt in der Klasse *TGAReader*. Sie implementiert, wie gesagt, das Interface *ImageReader*. Das Beispiel beschränkt sich auf den minimalen Aufwand, der zum Laden von Bildern über *ImageIO.read()* notwendig ist. Daher sind *getStreamMetadata* und *getImageMetadata* nur leere Hülsen – sie werden in diesem Zusammenhang nicht benötigt. Die Arbeit in dieser Klasse beschränkt sich im Großen und Ganzen darauf, den Header der Datei korrekt auszuwerten um eine passende *BufferedImage*-Instanz zu erzeugen. Anschließend bildet sie aus den enthaltenen Daten die korrekten Farbwerte, und die Methode *setRGB* fügt diese Werte an der richtigen Stelle in das Bild ein.

Das Beispiel kommt mit einem Ant-Build-Skript, das mittels des Target *makejar* eine JAR-Datei erstellt. Testen kann man die neu gewonnene Unterstützung für TGA-Bilder über das Ant-Target *run*. Vorher muss die JAR-Datei natürlich noch in das Verzeichnis für Extensions der benutzten Java-Laufzeitumgebung kopiert werden. Beim Start des Tests muss man Ant per *-Dimagefilename=<image.file>* den Namen einer zu ladenden TGA-Datei mitgeben. Der Vollständigkeit halber existiert noch das Ant-Target *run.old*. Es lädt Bilder über den angesprochenen Mechanismus in *java.awt.Toolkit*. Daher funktionieren hier trotz des neuen *ServiceProvider* keine TGA-Bilder.

Zum Schluss noch ein paar Worte zum Status des Beispiels: Der Code ist dafür gedacht zu lernen – er hat keine Produktionsreife erreicht. Das ergibt sich zum einen daraus, dass nicht alle TGA-Dateitypen unterstützt werden.

Zum anderen wurde der Code für das Parsing nicht auf Geschwindigkeit optimiert. Er soll lediglich zeigen, wie wenig Aufwand nötig ist, um ein neues Bildformat zu unterstützen. Interessierte Leser sind eingeladen, die bestehende Implementierung zu verbessern oder in der Folge dieses Artikels andere Implementierungen zu schaffen und damit vielleicht eine ausgereifte Bibliothek von unterschiedlichen *Image-Reader*n (oder vielleicht sogar *Image-Writer*n) zu schaffen. (ka)

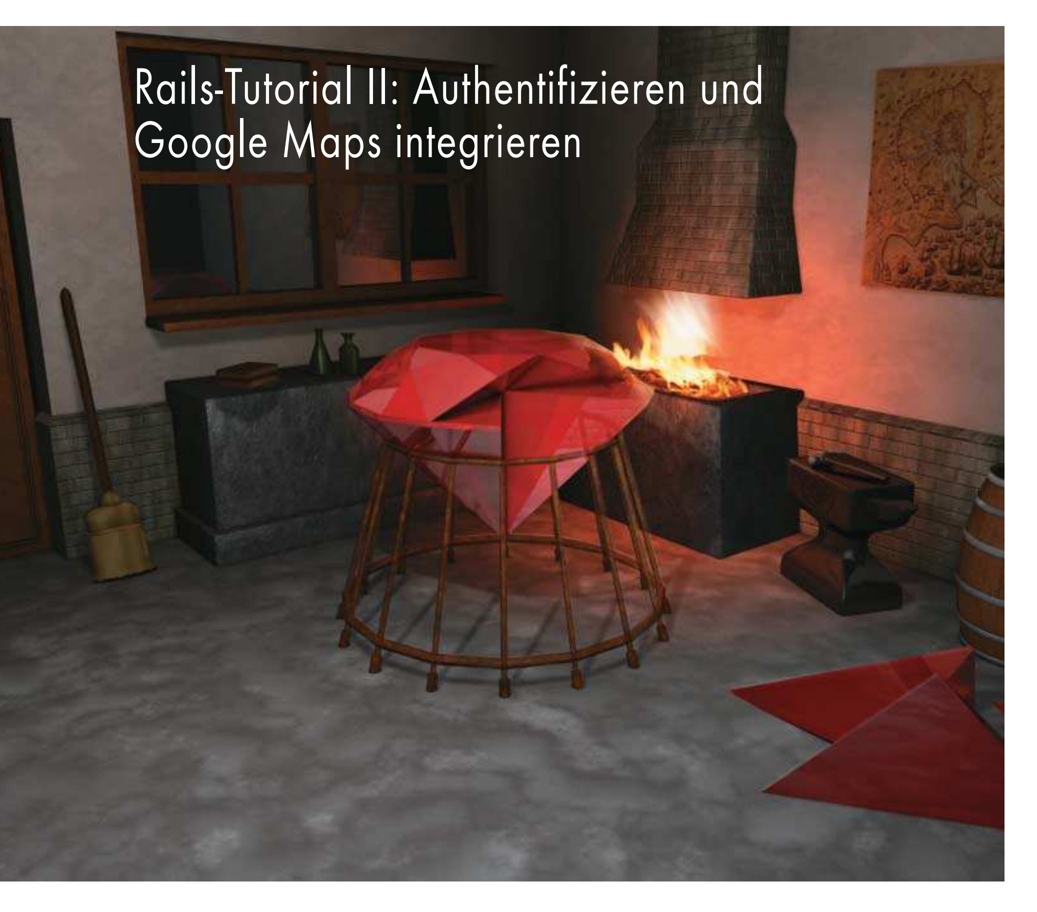
JÜRGEN KEY

ist Partner der Firma NetSys.IT. Als Senior-Softwaredesigner beschäftigt er sich mit allen Aspekten der Objektorientierung – von Analyse und Design bis Code Review.









Rails-Tutorial II: Authentifizieren und Google Maps integrieren

# In der Webschmiede

Denny Carl

Ruby on Rails unterstützt Entwickler bei vielen Aufgaben – sei es, eine Anwendung um Authentifizierung, Bilder, Thumbnails oder eine Google-Maps-Integration zu bereichern.

Im ersten Teil dieses Ruby-on-Rails-Tutorials ging es hauptsächlich darum, die Grundpfeiler der Rails-Anwendung Trainspotr zu entwickeln. Dazu zählt das Erstellen eines Layouts in HTML und CSS, das Erzeugen der Basis einer jeden Anwendung, das Hinterlegen der Datenbankparameter und das Implementieren erster Models, Controller sowie Views. Somit kann Trainspotr bisher Zugsichtungen aufnehmen, bearbeiten, anzeigen und löschen. Allerdings fehlt das Wichtigste: das Hinterlegen von Fotos samt automatischer Thumbnail-Erzeugung.

Nicht nur darum soll es in diesem Teil gehen. Durch Hinzufügen eines geschützten und eines Navigationsbereichs und das Integrieren einer Google Map bekommt die Anwendung nach und nach Community-Charakter. Technisch gesehen stehen das Arbeiten mit Assoziationen, das Erweitern einer Datenbanktabelle durch zusätzliche Migrations, Wert-Validierungen auf Model-Ebene, das Integrieren von Plug-ins und das Arbeiten mit der Rails-Konsole im Vordergrund.

## Zugangsbeschränkung mit HTTP Basic Auth

Es gibt verschiedene, teils komplexe Optionen, Teile einer Rails-Anwendung per Login und Passwort zu schützen. Diese werden meist durch das Hinzufügen eines Plug-in realisiert. Im Folgenden soll es um eine einfache, erst seit Kurzem zum Rails-Kern gehörende Variante dieser Funktion gehen. Sie basiert auf „HTTP Basic Auth“, die bislang meist im Zusammenhang mit einer *.htaccess*-Datei in Erscheinung getreten ist. In diesem Fall liegen Login-Name und Passwort in einer geschützten Datei auf dem Server. Der Benutzer gibt seine Kennung in ein browsereigenes Dialogfenster ein.

Es soll genügen, hier lediglich den eigentlichen Login-Mechanismus zu zeigen und auf ein Registrierungsformular zu verzichten. Der *Trainspots*-Controller soll durch ein Login geschützt sein und Funktionen werden nutzerabhängig umgestaltet. Das heißt, dass jeder Trainspotr-Nutzer nunmehr nur auf seine eigenen Zugsichtungen Zugriff erlangen darf. Die Benutzerdaten sollen in einer Datenbanktabelle enthalten sein.

Daher ist es zunächst erforderlich, der Anwendung ein neues Model hinzuzufügen. Dies erfolgt auf ähnliche Weise wie beim schon implementierten Model *Trainspot*: durch den Rails-Generator, der zudem eine Migration erzeugt. Die Felder *Login* und *Password*, beides String-Werte, sollen für das Model *User* ausreichen. Anschließend kann die Migration ausgeführt werden; es entsteht die Datenbanktabelle *users*.

```
ruby script/generate model User login:string ↵
                                password:string
rake db:migrate
```

Da in diesem Fall ein Registrierungsformular fehlt, mit dessen Hilfe Verwalter Benutzer anlegen können, muss eine andere Art des Einpflegens von Nutzerdaten erfolgen. Zunächst wäre hier ein Datenbank-Client zu nennen, mit dessen Hilfe Administratoren Datensätze und somit Login und Passwort ablegen können. Des Weiteren bietet sich ein Rails-Werkzeug an, das bei der Entwicklung einer Applikation vielfältige Dienste leisten kann – unter anderem zum Prototyping und zur Fehlersuche: die Konsole (aufzurufen mit *ruby script/console*).

Hierdurch kann man direkt mit der Rails-Anwendung interagieren, beispielsweise über die Kommandozeile mit den Models der Anwendung arbeiten und so einen neuen Benutzer anlegen. Nach dem Start der Konsole lässt sich direkt Ruby-Code eingeben. Die folgende Zeile erstellt einen Nutzer *test* mit einem gleichlautenden Passwort.

```
User.create(:login=>'test', :password=>'test')
```

In diesem Falle schreibt Active Record den neuen Datensatz direkt in die Tabelle *users*. An dieser Stelle sei darauf hingewiesen, dass das Speichern des Benutzerpassworts im Klartext, so wie es hier erfolgt, Risiken birgt und Administratoren eine Verschlüsselung mit MD5 oder ähnlichen Algorithmen in Betracht ziehen sollten. Plug-ins wie das beliebte *restful_authentication* beinhalten eine solche Verschlüsselung und bieten darüber hinaus einen kompletten Anmeldevorgang inklusive Mailversand an.

## Über Login und Passwort authentifizieren

Damit ist der Grundstein für die Zugriffsbeschränkung im *Trainspots*-Controller gelegt. Nun gilt es, ihn zu erweitern. Hierbei kommt wieder ein Filter zum Einsatz. Diesmal geht es nicht darum, eine Trainspot-Instanz zu erzeugen, sondern zu prüfen, ob der Zugang gewährt werden darf. Der Filter verweist auf eine Methode *authenticate* und soll alle Actions des Controllers außer *show* schützen. Die Action *TrainspotsControllers#show* soll später dazu dienen, das Anzeigen von Zugsichtungen für die gesamte Community zu ermöglichen. Die Pflege bleibt den jeweiligen Trainspottern vorbehalten.

Den Filter muss man dringend vor dem schon bestehenden Filter notieren, da die Authentifizierung an erster Stelle der Filter-Queue erfolgen soll. Das Attribut *except* gibt hier im Gegensatz zum schon bekannten *only* Ausnahmen an, für die der Filter nicht gelten soll.

```
class TrainspotsController < ApplicationController
  before_filter :authenticate, :except => [:show]
  ...
end
```

Prinzipiell kann die Methode *authenticate* innerhalb des *TrainspotsController* stehen. Allerdings sollten Entwickler davon ausgehen, dass sie später andere Controller zugriffsbeschränkt implementieren wollen. Im weiteren Verlauf dieses Teils des Tutorials soll das noch der Fall sein. Daher lohnt es sich, *authenticate* an einen zentralen Platz zu setzen, auf den alle Controller prinzipiell Zugriff haben.

Zu diesem Zweck eignet sich der *ApplicationController* hervorragend. Wie *TrainspotsController* erben alle Controller einer Rails-Anwendung von *ApplicationController*. Sein Quelltext befindet sich in *app/controllers/application.rb*.

In der Methode *authenticate* kommt die Authentifizierung per HTTP Basic Auth zum Einsatz. Dies erfolgt über die Methode *authenticate_or_request_with_http_basic* (siehe Listing 1). Sie erwartet einen Block mit dem eingegebenen Login-Namen und dem Passwort. Im Block können diese beiden Werte kontrolliert und verarbeitet werden. Programmierer können *ApplicationController#authenticate* als *protected* deklarieren; er ist so nur in den ableitenden Klassen einsetzbar.

In Listing 1 dient die Klassenmethode *authenticate* des *User*-Models dazu, das Ergebnis des Login-Vorgangs in *@current_user* festzuhalten. Der eigentliche Abgleich zwischen Eingaben und Datenbankinhalten findet dort statt, wo er hingehört: im Model. Die Methode gibt eine *User*-Instanz zurück, sollten die Angaben korrekt gewesen sein, oder *nil*, wenn keine Übereinstimmung vorhanden ist. In diesem Falle kommt es zu einer negativen Auswertung des Blocks, was den Zugang nicht gewährt. Die *User*-Instanz oder *nil* „landen“ in der Klassenvariable *@current_user*. Die steht nun allen von *ApplicationController* erbenden Klassen zur Verfügung. Sie kann zum Anzeigen von Nutzerdaten dienen oder als Entscheidungsgrundlage, ob ein *User* eingeloggt ist oder nicht.

**Listing 1: Authentifizierung I**

```
class ApplicationController < ActionController::Base
  ...
  protected
  def authenticate
    authenticate_or_request_with_http_basic do |login, password|
      @current_user = User.authenticate(login, password)
    end
  end
end
```

**Listing 2: Authentifizierung II**

```
class User < ActiveRecord::Base
  def self.authenticate(login, password)
    find_by_login_and_password(name, password)
  end
end
```

## Individuelle Zugsichtungen

Die Methode *User#authenticate* (siehe Listing 2) nutzt den dynamischen Finder *find_by_login_and_password*, um eine passende Instanz zu erzeugen. Mit *find_by_*… steht eine komfortable Variante zur Verfügung, bestimmte Datensätze auf Basis von Übereinstimmungen in frei wählbaren Feldern einer Datenbanktabelle zu finden.

Damit sollte ein freier Zugriff auf http://localhost:3000/trainspots nicht mehr möglich sein. Die Eingabe der Daten des Testbenutzers sind erforderlich.

Mit der rein zugriffsbeschränkenden Eigenschaft eines solchen Login geht eine weitere einher: Die feste Zuordnung eines Trainspot zu einem Benutzer. Jede Zugsichtung gehört genau zu einem Benutzer, wobei jeder mehrere Zugsichtungen erstellen und pflegen kann. Diese typische Relation zwischen Datenbanktabellen (1:n) lässt sich mit Active Record hervorragend abbilden. Mit Assoziationen erfolgt dies intuitiv, denn der Zusammenhang zwischen einzelnen Models lässt sich fast wortwörtlich – wenngleich auf Englisch – im Programmcode notieren.

Ein Benutzer hat viele Trainspots. Entsprechend schlägt sich das in *app/models/user.rb* nieder:

```
class User < ActiveRecord::Base
  has_many :trainspots
  ...
end
```

**iX-TRACT**

- Für Ruby on Rails existieren viele Plug-ins, die das Erstellen von Anwendungen erleichtern.
- Aufgaben wie die Benutzer-Authentifizierung oder das Einbinden von Bildern samt automatischer Vorschaubild-Erstellung lassen sich dank Plug-ins leicht lösen.
- Assoziationen und Validatoren sind weitere Hilfsmittel, die Trainspotr-Gemeinde zu schaffen.

Hinter *has_many* steht der Name des assoziierten Models in der Mehrzahl. Nun muss die Gegenseite, das Model *Trainspot*, über die Assoziation informiert werden. Dies erfolgt mit *belongs_to* und der Nennung des assoziierten Models in der Einzahl.

```
class Trainspot < ActiveRecord::Base
  belongs_to :user
end
```

Rein formal ist die Verbindung damit hergestellt, allerdings fehlt Active Record nun noch eine Möglichkeit, die Verknüpfung einzelner Datensätze zwischen den Datenbanktabellen überhaupt festzustellen und festzuhalten. Zu diesem Zweck muss das Model *Trainspot* und damit die Tabelle *trainspots* um eine Eigenschaft beziehungsweise Spalte erweitert werden, die einen Fremdschlüssel aufnimmt. Es handelt sich dabei um die ID des assoziierten Datensatzes, und es gilt: Die Tabelle, deren Model in der Relation den *belongs_to*-Part innehat, erhält diese Spalte. Per Rails-Konvention sollte sie mit dem Namen des verknüpften Models beginnen und mit *_id* enden. Somit ist die Tabelle *trainspots* um das Feld *user_id* zu erweitern.

Das erledigt eine Migration. Wenn der Dateiname dieser Migration gewissen Regeln folgt, muss ihr Inhalt nach deren Generierung nicht mehr verändert werden. Er sollte in diesem Fall mit *Add* beginnen und mit *To* und dem Namen des betreffenden Models enden; Binnenmajuskel bezeichnen den Anfang neuer Wörter. Dank des *Add* erzeugt Rails eine Migration, die lediglich Datenfelder zu einer bestehenden Tabelle hinzufügt. Bisher hat die Model-Generierung Migrations erzeugt, die mit *Create* begannen und somit einen Hinweis darauf gaben, dass Tabellen neu entstehen sollen.

```
ruby script/generate migration AddUserIdToTrain ↵
                                spot user_id:integer
rake db:migrate
```

Damit entsteht allerdings ein Problem, sollten schon Zugsichtungen in der Datenbank hinterlegt sein. Denn diese Datensätze haben zwar nun ein Feld *user_id*, allerdings ist es noch leer. Nun könnte man all diese Datensätze einfach löschen und im Benutzerkontext wieder anlegen. Oder man weist diese Datensätze nachträglich noch dem Testbenutzer zu. Letzteres erfolgt beispielsweise innerhalb einer Migration oder über die Konsole. Folgende Zeilen können Programmierer dort eingeben:

```
trainspots = Trainspot.find :all
user = User.find_by_login 'test'
trainspots.each { |trainspot|
  user.trainspots << trainspot
}
```

Dies verdeutlicht einen Vorteil der Assoziation: Mit *user.trainspots* – diese Eigenschaft entstand erst durch die *has_many*-Assoziation – erhält man Zugriff auf alle Trainspots, die mit einer bestimmten *User*-Instanz verknüpft sind. Mit dem Operator < kann man weitere hinzufügen. Dabei erhält das jeweilige Trainspot-Objekt die ID des Benutzers, die im neuen Feld *user_id* abgelegt wird. < schreibt diese Zuordnung sofort in die Datenbank.

Nun muss man noch den *Trainspots*-Controller anpassen. Er soll schließlich nur die Zugsichtungen anzeigen, bearbeiten und löschen können, die dem Nutzer gehören.

Hierbei kommt die aus Listing 1 bekannte Klassenvariable *@current_user* zum Einsatz. *before_filter* deklariert sie, bevor eine Action, die sie nutzen soll, ausgeführt wird.

In *TrainspotsController#index* kommt nun statt *@trainspots = Trainspot.find :all*, das benutzerunabhängig alle Zugsichtungen liefert, ein benutzerbezogenes Suchen zum Einsatz:

```
def index
  @trainspots = @current_user.trainspots.find :all
end
```

Das Erzeugen in *TrainspotsController#create* soll von nun an ebenfalls im Benutzerkontext erfolgen. Dies bedeutet, dass bei einer neuen Zugsichtung die Nutzer-ID des eingeloggten Benutzers zu speichern ist.

Die Methode *build* erzeugt eine Instanz des *Trainspot*-Models, die alle aus dem Eingabeformular kommenden Daten und darüber hinaus die passende Nutzer-ID enthält. Der restliche Vorgang der Action bleibt unberührt.

Weitere Actions des Controllers beziehen ihr *Trainspot*-Objekt dank des Filters, der auf *find_trainspot* verweist. Daher muss nur diese Methode noch geändert werden. So funktioniert DRY (Don't Repeat Yourself):

```
def find_trainspot
  @trainspot = @current_user.trainspots.find ↵
                                        (params[:id])
end
```

Da die Action *show* nicht benutzerbezogen arbeiten, sondern freien Zugriff gewähren soll, erhält sie einen Sonderstatus. Einerseits gilt für sie nicht mehr der Filter *find_trainspot*. Das Symbol *:show* muss deshalb aus dem Array des Attributs *only* im entsprechenden Filter verschwinden. Zudem erzeugt *TrainspotsController#show* ein Trainspot-Objekt unabhängig vom eingeloggten Benutzer.

```
def show
  @trainspot = Trainspot.find params[:id]
end
```

Um die Verwendung der Action *show* geht es im nächsten Teil des Tutorials, wenn die Gestaltung der Startseite im Mittelpunkt steht.

## Fotos hochladen und Thumbnails erstellen

Das Hochladen, Speichern und Verwalten von Fotografien der Zugsichtungen ist ein komplexes Thema, zumal das Anfertigen von Vorschaubildern ebenfalls auf der Wunschliste steht. Hier gilt es nach Werkzeugen zu suchen, die diese Funktion schon komplett anbieten. In Ruby on Rails erfolgt dies meistens über Plug-ins, die den Rails-Funktionsumfang erweitern. Meist ist lediglich das Herunterladen des Plug-in nötig, damit es einsatzbereit ist.

Die Rails-Allzweckwaffe für den Upload und das Verkleinern von Bilddateien ist das Plug-in *attachment_fu* (techno-weenie.net). Es benötigt eine Bildbearbeitungs-Bibliothek wie ImageMagick oder FreeImage, zudem ein passendes Ruby-Interface. Aus Gründen der Performance und Stabilität wird hier FreeImage in Verbindung mit ImageScience genutzt.

FreeImage zu installieren gestaltet sich dank Paketmanager unter Linux (etwa per *apt-get*) und Mac OS X (Macports) einfach. Windows-Nutzer laden sich das Binary von der Projektseite (freeimage.sourceforge.net) herunter und kopieren die DLL ins Unterverzeichnis *System32* der Windows-Installation. Anschließend kann man mit RubyGems ImageScience und davon abhängige Pakete installieren.

Der Unterschied zwischen einem Gem und einem Rails-Plug-in besteht hauptsächlich darin, dass Gems die

**Listing 3: Bildbeschreibung**

```
class Photo < ActiveRecord::Base
  has_attachment  :storage => :file_system,
    :max_size => 2.megabytes,
    :thumbnails => { :thumb => '80x80' },
    :processor => :ImageScience
  validates_as_attachment;
  belongs_to :trainspot;
end
```

**Listing 4: Controller der Fotos**

```
class PhotosController < ApplicationController
  before_filter :authenticate
  def new
    @trainspot = @current_user.trainspots.find(params[:trainspot_id])
  end

  def create
    @trainspot = @current_user.trainspots.find(params[:trainspot_id])
    @photo = @trainspot.photos.build(params[:photo])

    if @photo.save
      flash[:notice] = 'Foto wurde hochgeladen.'
      redirect_to trainspot_url(@trainspot)
    else
      render :action => :new
    end
  end
end
```

**Listing 5: Foto hochladen**

```
<h2>Foto für '<%= @trainspot.train %>' hochladen</h2>
<%= error_messages_for :photo %>
<% form_for(@photo, :url => trainspot_photos_url(@trainspot), :html => { :multipart => true }) do |f| %>
  <p>Bilddatei:<br />
  <%= f.file_field :uploaded_data %></p>
  <p><%= submit_tag "Hochladen" %></p>
<% end %>
```

Funktionen von Ruby erweitern, während Plug-ins Rails, genauer, die Anwendung, unter der das Plug-in installiert wurde, ergänzt. Die Installation erfolgt durch ein Skript: *ruby script/plug in install <URL>*. Es lädt die Dateien direkt vom Server des Anbieters herunter und platziert sie im Verzeichnis *vendor* der Anwendung, was für das spätere Deployment praktisch ist.

Das Plug-in speichert sämtliche Daten zu den Bildern (Format, Größe, Dateiname et cetera) in einer Datenbanktabelle und benötigt dazu ein eigenständiges Model. Neben den obligatorischen Feldern, die *attachment_fu* benötigt, wird noch ein weiteres aufgenommen: *trainspot_id*. Denn jedes Foto soll mit einer Zugsichtung verbunden sein, wobei eine Zugsichtung mehrere Fotos aufnehmen kann. Es handelt sich wieder um eine *has_many*-Assoziation.

```
ruby script/generate model Photo filename:string ⮐
      content_type:string size:integer width:integer ⮐
  height:integer parent_id:integer thumbnail:string ⮐
                                trainspot_id:integer
rake db:migrate
```

Das Feld *parent_id* ist nötig, weil *attachment_fu* zwischen den selbst erzeugten Thumbnails und diesem Model und damit zum Originalbild einen Bezug herstellt. Da ein Bild mehrere unterschiedlich dimensionierte Thumbnails besitzen kann, muss das Feld *thumbnail* sein, in dem die Bezeichnung des jeweiligen Thumbnail zu liegen kommt.

Nun muss man das *Photo*-Model so erweitern, dass es *attachment_fu*-kompatibel ist. *has_attachment* legt fest, wie groß das Thumbnail eines Fotos sein darf. Ein Validator – mehr dazu weiter unten – überprüft, ob die Datei, die hochzuladen ist, den Anforderungen entspricht. Bei dieser Gelegenheit kann man die Relation zum Model *Trainspot* notieren.

Hierdurch nimmt das System, wie Listing 3 zeigt, Bilddateien bis maximal 2 MByte entgegen und speichert diese im Dateisystem. Alternativ können die Bilder in einer Datenbank oder bei Amazons S3 liegen. Nach dem Hochladen erstellt Rails pro Foto ein Thumbnail – als *thumb* bezeichnet und maximal 80 × 80 Pixel groß.

Um das Model zu nutzen, ist wieder ein Controller anzulegen. Hierbei soll es genügen, wenn dieser lediglich das Anlegen neuer Fotos berücksichtigt. Das erfordert die Actions *new* und *create*:

```
ruby script/generate Controller Photos new create
```

Vor dem Fertigstellen des *Photos*-Controllers steht eine Überlegung an, die die Frage beantwortet, wie sich Fotos optimalerweise im Gesamtkontext der Anwendung eingliedern sollen. Zugsichtungen „versteht“ diese Anwendung als Ressourcen. Fotos, von denen es pro Zugsichtung mehrere geben kann, sind demnach Unterressourcen einer Trainspot-Ressource. Dies lässt sich dank des Rails-Routings und des REST-Ansatzes leicht umsetzen. Dazu wird in diesem Falle an *map.resources :trainspots* einfach ein Block angehängt, wobei die Blockvariable stellvertretend für die übergeordnete Ressource steht.

```
map.resources :trainspots do |trainspot|
  trainspot.resources :photos
end
```

Dadurch entstehen saubere, leicht zu konstruierende URLs. Beispielsweise ist /trainspots/1/photos/new die URL zum Hochladen eines neuen Fotos, das zur Zugsichtung mit der ID 1 gehören soll.

Der Quelltext der beiden Actions des *Photos*-Controllers enthält wenig Neues. Lediglich die Berücksichtigung der Oberressource muss hier erfolgen. Die ID des entsprechenden Trainspots liegt per Konvention in *params[:trainspot_id]* vor. Darauf basierend wird das passende *Trainspot*-Objekt erzeugt, das wiederum lediglich aus dem Bestand des eingeloggten Benutzers stammen darf. Dies deutet schon an, dass auch *PhotosController* zugriffsbeschränkt ist. Der auf *ApplicationController#authenticate* zugreifende Filter eröffnet die Klassendeklaration (siehe Listing 4).

Auf View-Ebene ist nun noch ein Formular zu erstellen, das den Namen der hochzuladenden Datei aufnimmt und an den Server übergibt. Es findet in *app/views/photos/new.html.erb* Platz (siehe Listing 5).

Durch das Einbinden der Ressource *photos* als Unterressource stehen dem Entwickler besondere Named Routes, sogenannte Nested Routes zur Verfügung. Hier kommt beispielsweise die URL *trainspot_photos_url* zum Tragen. Sie erzeugt den Pfad zur Ressource *photos*, der die dazugehörige *trainspots*-Ressource beinhaltet.

Über den Parameter *html* kann man HTML-Attribute an den *form*-Tag übergeben, den der Rails-Helper *form_for* erzeugt. Da es hier um das Hochladen einer Datei geht, muss *multipart* den Wert *true* haben.

*attachment_fu* erwartet, dass die Informationen zur hochzuladenden Datei als *uploaded_data* übergeben werden. Daher ist diese Bezeichnung beim Helper *file_field* anzugeben.

Nicht zu vergessen ist die vollständige Implementierung der Assoziation *Trainspot/Photo*. Das Trainspot-Model muss dazu noch durch *has_many* erweitert werden:

```
class Trainspot < ActiveRecord::Base
  belongs_to :user
  has_many :photos
end
```

Im Trainspots-View *index.html.erb* (siehe Listing 6) kann nun ein Link hinterlegt sein, der das Hochladen eines Fotos ermöglicht. Das Skript erweitert einfach die Spalte, die bisher die Links „Anzeigen“, „Bearbeiten“ und „Entfernen“ enthält, um „Fotos hochladen“. Dazu dient die Nested Route *new_train spot_photo_path(trainspot)*, wobei ein Parameter ein weiteres Mal auf die Oberressource verweist.

## Vorschau durch Thumbnails anzeigen

Nun kann ein erster Testlauf des *Photos-Controller* starten. Bei korrektem Verlauf befindet sich im *public*-Verzeichnis der Rails-Anwendung ein Verzeichnis *photos*, in dem Originalbilder und Thumbnails in Unterverzeichnissen vorliegen.

**Listing 6: Link zum Bildladen**

```
<!-- ... -->
<td>
  <%= link_to 'Anzeigen', trainspot %> |
  <%= link_to 'Bearbeiten', edit_trainspot_path(trainspot) %> |
  <%= link_to 'Entfernen', trainspot, :confirm => 'Sind Sie sicher?', :method => :delete %> |
  <%= link_to 'Fotos hochladen', new_trainspot_photo_path(trainspot) %>
</td>
<!-- ... -->
```

Im *index*-View des *Trainspot*-Controllers soll nun das jeweils erste Thumbnail einer Zugsichtung erscheinen. Dazu muss der Entwickler zunächst das Model *Trainspot* um eine Methode erweitern, die eben dieses erste Foto in Form einer entsprechenden Instanz des Models *Photo* ausgibt. Dies erfolgt über die Klassenmethode *find* und die Angabe *:first*. Das Objekt *photos* wird dank der Assoziation zur Verfügung gestellt und enthält alle Instanzen des *Photo*-Models, die eine Verbindung zur *Trainspot*-Instanz haben.

```
class Trainspot < ActiveRecord::Base
  belongs_to :user
  has_many :photos
  def first_photo
    photos.find :first
  end
end
```

In *app/views/trainspots/index.html.erb* kann nun die HTML-Tabelle um eine Spalte erweitert werden – um die „Vorschau“ (siehe Listing 7). Der Rails-Helper *image_tag* bindet das erste Foto, so es denn schon eins gibt, als Thumbnail ein und verlinkt ihn zudem, indem er auf die Action *show* des *Trainspots-Controllers* verweist. Dazu genügt die *Trainspot*-Instanz als Sprungziel. Rails „weiß“, was der Entwickler damit erzielen möchte.

Zur Anzeige der Vorschau prüft die Anwendung zunächst, ob es Fotos gibt. Ist dies der Fall, bestimmt die Methode *public_filename*, durch *attachment_fu* ins Spiel gekommen, über einen Parameter, ob ein und wenn ja, welches Thumbnail zur Anzeige kommen soll.

Der View *show.html.erb* des Trainspots-Controllers soll nun alle Fotos einer Zugsichtung zeigen und bei einem Klick auf ein Thumbnail das dazugehörige Originalbild öffnen. Die Fotos eines *Trainspot*-Objekts liegen in dessen Eigenschaft *photos* vor. Es handelt sich dabei um ein Array. Jedes Array-Element soll angezeigt werden, für jedes muss deshalb HTML-Code vorhanden sein, der sich bis auf die Dateinamen gleicht. Daher kann ein Partial die Angelegenheit „DRYer“ gestalten.

Zur Erinnerung: Die schon im ersten Tutorialteil erwähnten Partials sind wiederverwendbare Teil-Views, deren Dateinamen mit einem Underscore beginnen – eine Rails-Konvention.

Hier kommt eine weitere Fähigkeit von Partials zum Einsatz. Man kann ein Array an ein Partial übergeben und Rails stellt das Partial automatisch für jedes Array-Element dar: für jede *Photo*-Instanz. Ähnlich einer Schleife, mit der man diesen Stolperstein umgehen könnte. Innerhalb des Arrays steht das jeweilige *Photo*-Objekt in Form einer lokalen Variablen zur Verfügung. Diese heißt genau wie das Partial – aber ohne Underscore.

Unter *app/views/trainspots/_thumbnail.html.erb* liegt das Partial. Somit zeigt innerhalb des Partials die Variable *thumbnail* auf eine *Photo*-Instanz.

```
<%= link_to
image_tag(thumbnail.public_filename(:thumb)),
thumbnail.public_filename %>
```

Bei Nutzung der Methode *public_filename* des *Photo*-Objekts ohne Parameter wird einfach der Dateiname inklusive Pfad der Originaldatei ausgegeben. In diesem Falle führt das durch die Verwendung in einem *link_to*-Helper zur Anzeige des Originalbildes. Das Template *app/views/trainspots/show.html.erb* wird nun entsprechend ergänzt (siehe Listing 8).

Damit ist der Bereich Hochladen von Fotos und das Anfertigen von Thumbnails beendet. Auf typische Rails-Art setzen ein Plug-in und wenige Codezeilen dies um. Ähnlich verhält es sich mit einer weiteren Funktion von Trainspotr: das Anzeigen einer Google Map, die die Fotoposition zeigt.

## Google Maps einbinden

Zunächst soll das *Trainspot*-Model zwei weitere Felder bekommen, die Längen- und Breitengrad der Fotoposition speichern sollen. Mit einer Migration sind zwei Felder, die Kommawerte speichern können, schnell angelegt.

```
ruby script/generate migration AddLngAndLatTo ⁊
        Trainspot lng:float lat:float
rake db:migrate
```

Da das Formular zum Anlegen und Bearbeiten einer Zugsichtung als Partial in *app/views/trainspots/_form.html.erb* ausgelagert ist, gibt es nur eine Stelle für zwei Actions, an der die beiden Felder hinzugefügt würden müssen.

```
<p>Breitengrad<br />
<%= f.text_field :lat %></p>
<p>Längengrad<br />
<%= f.text_field :lng %></p>
```

Bei der Visualisierung dieser Koordinaten soll ein Plug-in namens YM4R/GM helfen, das das Nutzen von Google Maps ohne die Verwendung von Javascript ermöglicht. Um es einsetzen zu können, muss gegebenenfalls ein Subversion-Client installiert sein, denn es wird bei der Installation direkt aus einem SVN-Repository gelesen.

```
ruby script/plugin install svn://⁊
        rubyforge.org/var/svn/ym4r/⁊
        Plugins/GM/trunk/ym4r_gm
```

Im Hintergrund arbeitet selbstverständlich Javascript. Daher muss man die entsprechenden Dateien zunächst im Head-Be-

**Listing 7: Erweiterte HTML-Tabelle**

```
<h2>Zugsichtungen</h2>
<table>
  <tr>
    <th>Zug oder Lok</th>
    <th>Ort der Aufnahme</th>
    <th>Datum und Zeit</th>
    <th>Bemerkungen</th>
    <th>Vorschau</th>
    <th></th>
  </tr>

  <% for trainspot in @trainspots %>
  <tr>
    <td><%= h trainspot.train %></td>
    <td><%= h trainspot.location %></td>
    <td><%= h trainspot.date %></td>
    <td><%= h trainspot.notes %></td>
    <td>
      <% unless trainspot.photos.blank? %>
        <%= link_to image_tag(trainspot.first_photo.public_filename(:thumb)), trainspot %>
      <% end %>
    </td>
    <td>
      <%= link_to 'Anzeigen', trainspot %> |
      <%= link_to 'Bearbeiten', edit_trainspot_path(trainspot) %> |
      <%= link_to 'Entfernen', trainspot, :confirm => 'Sind Sie sicher?', :method => :delete %> |
      <%= link_to 'Fotos hochladen', new_trainspot_photo_path(trainspot) %>
    </td>
  </tr>
  <% end %>
</table>
<p><%= link_to 'Neue Zugsichtung anlegen', new_trainspot_path %></p>
```

**Listing 8: Foto vergrößern**

```
<% unless @trainspot.photos.blank? %>
  <p><b>Fotos:</b> (Klicken zum Vergrößern)<br />
  <%= render :partial => 'thumbnail', :collection => @trainspot.photos %>
<% else %>
  <p>Es sind noch keine Fotos hinterlegt worden.</p>
<% end %>
```

**Listing 9: Längen-/Breitengrad einbinden**

```
def show
  @trainspot = Trainspot.find params[:id]
  @map = GMap.new("map_div_id")
  @map.control_init(:large_map => true, :map_type => true)
  @map.center_zoom_init([@trainspot.lat, @trainspot.lng], 15)
  marker = GMarker.new([@trainspot.lat, @trainspot.lng], :title => @trainspot.train, :info_window => @trainspot.notes)
  @map.overlay_init(marker)
end
```

**Listing 10: Partial mit @current_user**

```
<% if @current_user %>
  Eingeloggt als <%= @current_user.name %>
<% else %>
  Sie sind nicht eingeloggt.
<% end %>
<ul>
  <li><%= link_to 'Startseite', root_path %></li>
<% if @current_user %>
  <li><%= link_to 'Alle eigenen Zugsichtungen', trainspots_path %></li>
  <li><%= link_to 'Neue Zugsichtung', new_trainspot_path %></li>
<% else %>
  <li><%= link_to 'Login', trainspots_path %></li>
<% end %>
</ul>
```

reich des Layouts einbinden. Das Plug-in stellt dazu den Helper *<%= GMap.header %>* zur Verfügung. Sollten Entwickler YM4R/GM auf einer Website einsetzen, die nicht lokal auf dem eigenen Rechner läuft, ist das Erzeugen eines eigenen Schlüssels für die Nutzung der Google Maps API unumgänglich. Den erzeugten Schlüssel kann man im Attribut *:key* der Methode *GMap#header* als String-Objekt übergeben.

Als Nächstes ist *TrainspotsController#show* anzupassen, der Vorbereitungen für das Anzeigen der Karte treffen soll, indem er beispielsweise bestimmt, welcher Kartentyp verwendet werden, welche Koordinaten die Mitte der Karten haben und wie stark der Zoom sein soll. Darüber hinaus erzeugt er einen Marker, der den Zug- oder Lokbezeichner und Bemerkungen anzeigen soll. Alles liegt in einer Instanz der Klasse *GMap* und ist in *@map* gespeichert. Es handelt sich um eine Instanzvariable, da *@map* so auch im View verfügbar ist (siehe Listing 9).

Im dazugehörigen Template fehlen nun noch zwei Zeilen, die das Anzeigen der Map durch das Erzeugen des Markup und Javascript regeln. Dabei soll ein *div*-Element mit der Breite und Höhe von 500 Pixeln den Rahmen der Karte bilden:

```
<p><b>Position:</b>
<%= @map.to_html %>
<%= @map.div(:width => 500, :height => 500) %>
```

## Validierung der Schreibzugriffe

Abschließend muss man noch sicherstellen, dass stets Längen- und Breitengrade angegeben werden. Zu diesem Zweck gibt es Validatoren in Rails. Sie überprüfen bei jedem Schreibzugriff auf die Datenbank, ob alle zum Speichern erforderlichen Voraussetzungen erfüllt sind. Ist dies nicht der Fall, bricht Rails den Schreibzugriff ab und erzeugt Fehlermeldungen.

Um zu prüfen, ob Längen- und Breitengrade vorhanden und numerisch sind, können die Validatoren *validates_presence_of* und *validates_numericality_of* im Model *Trainspot* zum Einsatz kommen. Es gibt noch viele weitere, die beispielsweise ein bestimmtes Format oder die Übereinstimmung mit einem Wert aus einem Array prüfen. Mehr dazu enthält die API-Dokumentation von Rails.

Außer den Geodaten prüfen die Validatoren das Vorhandensein der Zugbezeichnung und des Ortes (in Worten). Ob es sich bei den übergebenen Werten um Zahlen handelt, spielt lediglich bei Längen- und Breitengrad eine Rolle.

Zum Abschluss dieses Teils des Tutorials soll es noch um den Navigationsbereich auf der linken Seite der Oberfläche gehen. Man könnte die Navigationslogik direkt in das Layout bauen, da die Navigation auf jeder Seite benötigt wird. Aber auch hier lohnt die Modularisierung durch ein Partial.

Da das Navigations-Partial zu keinem Controller gehört, sondern überall gebraucht wird, erstellen Rails-Entwickler ein eigenes Verzeichnis *shared* innerhalb des Views-Verzeichnisses. Im Layout kann das Partial den bisherigen Platzhalter (*NAV*) ersetzen:

```
<%= render :partial => 'shared/navigation' %>
```

Das Partial selbst macht sich *@current_user* zueigen, das dank der Erzeugung in *ApplicationController* in jeder Situation auf View-Ebene zur Verfügung steht. Dadurch kann ein Navigationsmenü angeboten werden, das berücksichtigt, ob ein Nutzer eingeloggt ist oder nicht (siehe Listing 10).

Der Link zur Startseite steht allen Nutzern zur Verfügung. Das Sprungziel wird dabei durch die Route *root* bestimmt, die wiederum auf den *HomeController* zeigt. Beim Login-Link wurde ein bisschen geschummelt, denn er zeigt auf die Übersicht aller Zugsichtungen. Da aber zuvor ein Eingeben von Benutzername und Passwort erforderlich ist, erfüllt der Link seinen Zweck.

**Tutorialinhalt**

| | |
|---|---|
| Teil I: | Einrichten der Umgebung, Aufbau des Grundlayouts der Website sowie Model, Controller und View für das Anlegen und Bearbeiten von Loksichtungen |
| **Teil II:** | **Anlegen eines geschützten Bereichs mit Registrierung, Bilder laden und Thumbnails generieren** |
| Teil III: | Startseite mit Fotos aus dem Datenbestand und Ajaxifizieren der Oberfläche mit Bewertung der Fotos. Hinweise zum Deployment |

## Fazit

Trainspotr hat auf den zurückliegenden Seiten viel an Funktionsumfang gewonnen. Durch das Einbinden von Plug-ins und das Nutzen von Assoziationen, Validatoren und Migrations hat Rails dabei geholfen, dass dies schnell und unkompliziert vonstatten ging. Das automatische Erstellen von Thumbnails und die Anzeige einer Google Map mit Markern waren dank der komfortablen Plug-in-Funktion von Rails mit wenigen Handgriffen erledigt.

Der momentane Funktionsumfang der Applikation kann unter www.trainspotr.de ausprobiert werden. Dort und auf dem *iX*-FTP-Server steht auch der Quellcode zum Download zur Verfügung.

Im nächsten und letzten Teil erhält die Anwendung ihren Feinschliff. Dabei entstehen die Startseite von Trainspotr, sowie einige Funktionen, die den durch die Trainspotter erzeugten Datenbestand nutzen. Ein Bewertungssystem auf Basis von Ajax kommt hinzu. Zudem werden Hinweise zum Testen einer Rails-Anwendung sowie des Deployment gegeben. (hb)

DENNY CARL

ist seit 2001 selbstständiger Webdesigner und -entwickler in Berlin.



Distributed Shell

# Herrscher aller Reußen

**Udo Seidel**

Muss der Administrator auf mehreren Rechnern dieselben Befehle ausführen, kann er notfalls auf *for*-Schleifen oder selbst gebastelte Skripte zurückgreifen. Bequemer geht es jedoch mit einem geeigneten Werkzeug wie der Distributed Shell *dsh*.

Verwaltet der Administrator Hunderte von Rechnern, ist die Aufgabe ohne Hilfsmittel nicht mehr zu bewältigen. Spezielle Managementsoftware hilft, belastet jedoch das Budget. Außerdem erfordern die gängigen Lösungen Installationen auf jedem einzelnen Rechner. Beides kann man mit der Distributed Shell *dsh*, auch bekannt als „Dancer’s Shell“, umgehen (siehe Kasten „Onlinequellen“).

Wer das Programm selbst kompilieren möchte, muss nacheinander die Pakete *libdshconfig* und *dsh* herunterladen und auf dem Administrationsrechner installieren. Manche Linux-Distributionen, darunter Debian, liefern kompilierte Pakete mit.

Als Transportmittel kann *dsh* die Secure Shell *ssh* oder die Remote Shell *rsh* verwenden – aus Sicherheitsgründen empfiehlt sich Erstere. Auf der Kommandozeile kann der Nutzer sie mit *–r ssh* auswählen. Tippfaule tragen die Zeile *remoteshell=ssh* in die *dsh*-Konfigurationsdatei ein, die normalerweise auf den Namen */etc/dsh/dsh.conf* hört. Nutzer können individuelle Einstellungen in *~/.dsh/dsh.conf* vornehmen.

Zusätzlich benötigt *dsh* ein „Inventar“: eine Liste aller zu administrierenden Rechner. Zwar kann man sie mit *–m rechner,rechner,…* auf der Kommandozeile übergeben. Üblicherweise legt man sie jedoch in */etc/dsh/machines.list* ab. Die Syntax *user@rechner* und die Verwendung von IP-Adressen statt Rechnernamen sind ebenfalls zulässig.

Ruft man *dsh –a “uname –r“* auf, klappert *dsh* alle Rechner nacheinander ab, loggt sich ein und führt den Befehl aus. Die Fragen nach dem jeweiligen Passwort kann man zum Beispiel durch Eintragen des Admin-Rechners in *.rhosts* unterbinden. Bei *ssh* sollte der Administrator lieber ein sichereres Verfahren auf Schlüsselbasis verwenden.

Klappt das Einloggen ohne Passwort-Abfrage, kann man mit der Option *–c* die Rechner parallel arbeiten lassen. Um die Last auf dem Admin-Rechner in Grenzen zu halten, sollte man jedoch mit *–F <maximum>* die Zahl der gleichzeitig laufenden Prozesse begrenzen. Mit *waitshell=0* und *forklimit=<maximum>* lassen sich beide Angaben in der Konfigurationsdatei verewigen.

### Onlinequellen

| | |
|---|---|
| Dancer’s Distributed Shell | www.netfort.gr.jp/~dancer/software/dsh.html.en |
| Multihost SSH Wrapper | sourceforge.net/projects/mussh/ |
| Clusterssh | clusterssh.wiki.sourceforge.net/Main+Page |
| Global Shell | outflux.net/unix/software/gsh/ |
| mass.pl | www.lerp.com/~sic/mass/ |
| Tentakel | tentakel.biskalar.de |
| Clusterit | www.garbled.net/clusterit.html |

Soll nur ein Teil der Rechner eine Aufgabe durchführen, kann der Nutzer Gruppen definieren. Dazu muss er lediglich die Namen der Mitglieder in */etc/dsh/group/<gruppenname>* oder *~/.dsh/group/<gruppenname>* eintragen. Anschließend kann er etwa mit *dsh –g linux-pcs “<kommando>“* ein Kommando nur auf den vorhandenen Linux-Rechnern ausführen lassen.

Bei paralleler Ausführung mit *–c* erscheinen die Ausgaben der einzelnen Rechner bunt durcheinandergewürfelt auf dem Schirm. Benötigt der Nutzer etwas mehr Übersicht, kann er *dsh* mit der Option *–M* oder *showmachinenames=1* in der Konfigurationsdatei anweisen, jeder Ausgabe den Namen des Rechners voranzustellen, von dem sie stammt. Stören die Zusätze – etwa beim maschinellen Nachbearbeiten – kann man sie mit *–H* ausschalten.

## Adelige, Bauern und Knechte

In größeren Netzen dauern das Verbreiten des Kommandos und das Einsammeln der Ergebnisse entsprechend länger. Daher erlaubt es *dsh*, die Arbeit zu delegieren. Allerdings muss dazu das Programm auf allen Rechnern installiert sein, weil der Nutzer die Relay-Stationen nicht frei wählen kann. Lediglich die Zahl der Helfer kann er mit *–N <nummer>* einstellen.

Es gibt eine Reihe von Skripten mit vergleichbarer Funktion. SSH-Kenner finden beim Multihost SSH Wrapper *mussh* viele bekannte Optionen wieder. Wer Perl bevorzugt, wird bei *clusterssh*, der Global Shell *gsh* oder *mass.pl* fündig, Python-Fans bei *Tentakel*. Alle arbeiten ähnlich wie *dsh* mit einem Inventar und *ssh* oder *rsh*.

Außerdem lohnt es sich, einen Blick auf die Werkzeugsammlung von *clusterit* zu werfen. Sie enthält ebenfalls eine *dsh*, deren Aufrufsyntax jedoch von der beschriebenen abweicht. Außerdem gehören zum Paket das Programm *barrier*, mit dem sich die Prozesse auf den einzelnen Rechnern synchronisieren lassen. *jsh* und *jsd* unterstützen ein einfaches Job-Scheduling. (mr)

DR. UDO SEIDEL

leitet eine Unix/Linux-Sysadmin-Gruppe bei der Amadeus Data Processing GmbH in Erding.






Eine Institution im deutschsprachigen Fernsehen

# Tatort

## Kai König



Am 25. Mai 2008 hat die ARD den 700. Kriminalfilm aus der Reihe Tatort ausgestrahlt. Ein Grund, der Serie und ihrem Hintergrund im Netz auf die Spur zu kommen.

Das Erfolgsrezept der im Ersten ausgestrahlten Serie Tatort beruht unter anderem auf der Tatsache, dass es eine Vielzahl von Ermittlerteams gibt. Diese sind in verschiedenen Städten angesiedelt und prägen die Krimireihe durch Lokalkolorit sowie regionalen Humor und Besonderheiten. Als offizieller Einstiegspunkt zur Tatort-Recherche im Web bietet die Seite der ARD (www.daserste.de/tatort) dem interessierten Surfer eine Vielzahl weiterführender Informationen.

Empfehlenswert ist beispielsweise die Kommissar-Übersicht auf www.daserste.de/tatort/kommissare.asp. Hier wird anschaulich visualisiert, in welchen Städten die aktuellen Ermittler beheimatet sind, welches ihre letzten Fälle waren, und man erhält sogar Querverweise zu Auftritten der Schauspieler in anderen ARD-Sendungen wie Talkshows.

Anhand dieser Karte stößt man beispielsweise auch auf den österreichischen Tatort-Kommissar Major Moritz Eisner, gespielt von Harald Krassnitzer (de.wikipedia.org/wiki/Harald_Krassnitzer). Die vom ORF produzierten Episoden stehen bei einigen der regelmäßigen Zuschauern allerdings im Ruf, Tourismus-Werbung ohne Handlung zu sein. So sehen es beispielsweise die „Milchjunkies“ (milch.junkies.ws/2007/05/20/revolution-beim-tatort-osterreich/).

Noch vor wenigen Jahren beteiligte sich auch das Schweizer Fernsehen erfolgreich an der Produktion der Tatort-Reihe. 2001 hat es damit aufgehört – mit der Begründung, dass es die Produktionsmittel in andere Formate überführen wolle. Das Schweizer Fernsehen produzierte in 12 Jahren Tatort 12 Episoden, wie sich der Liste der ehemaligen und aktuellen Tatort-Ermittler auf Wikipedia entnehmen lässt (de.wikipedia.org/wiki/Tatort_(Fernsehreihe)#Liste_der_aktuellen_Tatort-Ermittler). Auf der privaten und unglaubliche Details bietenden Seite tatort-fundus.de wurde im Februar 2008 spekuliert, ob die Schweiz in den Tatort-Verbund zurückkehren werde, da man sich an der Produktion eines in Deutschland als Tatort gesendeten Krimis beteiligt hatte. In der Schweiz lief die Produktion allerdings nur als normaler TV-Film (www.tatort-fundus.de/web/index.php?id=3254).

Das wirft die Frage auf, wie man einen Krimi als Tatort identifizieren kann. Am einfachsten dürfte das über die einprägsame Titelmelodie und den Vorspann gelingen. Jedes Kind in Deutschland kennt beide wahrscheinlich von Sonntagabenden im Wohnzimmer der elterlichen Wohnung – oder zumindest die Musik, die auch im Bett des Kinderzimmers zu hören ist. Wer schon lange keinen Tatort mehr gesehen hat – den Vorspann gibt es auf Youtube unter www.youtube.com/watch?v=veOJYxHlgW8.

## Die Augen im Hintergrund

Ein wenig tiefergehende Forschung auf der gleichen Seite fördert die Tatsache zutage, dass es verschiedene Versionen von Vor- und Abspann zu geben scheint. Die Titelmusik, komponiert von Klaus Doldinger, wurde im Laufe der Zeit nur zweimal leicht angepasst, allerdings erkennt man in neueren Versionen des Vorspanns ein klareres Bild, was vermutlich auf digitale Nachbearbeitung des Originalmaterials zurückzuführen ist. Die flüchtende Person im Vorspann hat übrigens der Schauspieler und heutige Beleuchtungstechniker Horst Lettenmayer gespielt. Ihm gehören auch die im Trailer zu sehenden Augen. In einem Interview mit der Zeitung „Die Welt“ erfährt man ein wenig mehr zu dieser an sich im Hintergrund stehenden Person: www.welt.de/fernsehen/article2026467/Die_bekanntesten_Augen_des_Tatorts.html.

Dem Tatort wird nachgesagt, dass die Reihe, sofern in der nötigen Vorlaufzeit möglich, auf aktuelle gesellschaftliche und politische Begebenheiten eingeht. Das war von Anfang an der Fall, denn schon der erste Tatort vom NDR im Jahre 1970 mit dem Titel „Taxi nach Leipzig“ sorgte für Aufsehen hinsichtlich der Darstellung des deutsch-deutschen Verhältnisses. Eine ausführliche Rezension mit Bildern (wie auch zu anderen Episoden) findet man auf der Seite tatort-fans.de unter tatort-fans.de/tatort-001-taxi-nach-leipzig/. Seit April diesen Jahres ist dieser Krimi auch als Buch in der Reihe „Sittengeschichte Deutschlands“ erhältlich (www.amazon.de/Taxi-nach-Leipzig-Sittengeschichte-Deutschlands/dp/3936791473?ie=UTF8&s=books&qid=1211660082&sr=1-1).

## Unvergessene Ermittler

Neben herausragenden Folgen gibt es herausragende Ermittler. Unvergessen das Duisburger Duo Schimanski und Thanner (Götz George und Eberhard Feik) oder der Essener Kommissar Heinz Haferkamp, gespielt vom leider im letzten Jahr verstorbenen Hansjörg Felmy. Das aktuelle Team des WDR-Tatorts bestehend aus Ballauf und Schenk gibt ebenfalls eine gute Figur ab und bekommt auf zahlreichen Fanseiten Bestnoten. Der WDR hat also bei der Besetzung der Rollen ein glückliches Händchen bewiesen, allerdings finden sich auch in anderen Städten und Ländern erfolgreiche Kommissare. Der Südwestdeutsche Rundfunk hat beispielsweise mit dem Duo Lena Odenthal und Mario Kopper die zurzeit dienstältesten Ermittler im Einsatz (seit 1989), dicht gefolgt von Batic und Leitmayr aus München (seit 1991).

Wie angedeutet spiegeln sich im Tatort Zeitgeist und die Entwicklung der deutschen Gesellschaft wider. Michelle

Mattson hat diese Tatsache wissenschaftlich untersucht und die Ergebnisse unter dem Titel „Tatort: The Generation of Public Identity in a German Crime Series“ veröffentlicht (www.jstor.org/pss/488458). Eine weitere Quelle mit interessanten Hintergrundinformationen zu Aufbau und Planung der Krimi-Reihe ist das Interview mit Gebhard Henke vom WDR, der unter anderem bei der ARD als „Tatort-Koordinator“ agiert (www.tatort-fundus.de/web/index.php?id=226).

Ein relativ neues Konzept im Tatort sind die Crossover-Handlungen. Darunter versteht man Episoden, in denen Kommissare aus einer bestimmten Stadt in einem anderen Ort ermitteln müssen und dabei auf die dort beheimateten Tatort-Ermittler treffen. Dieses Konzept stammt ursprünglich aus US-amerikanischen TV-Sendungen (beispielsweise „Buffy“ und „Angel“) und wurde in den neueren Tatort-Folgen bei zwei Gelegenheiten mit gegenseitigen Besuchen der Leipziger und Kölner Kommissare aufgegriffen.

Des Weiteren gibt es Crossovers mit Polizeiruf 110, einer schon in der DDR bekannten und beliebten Krimiserie. 1990 trafen die damaligen Ruhrpott-Kommissare Schimanski und Thanner auf ihre Polizeiruf-Pendants; ein weiterer Versuch brachte im Jahr 2006 das Frankfurter Tatort-Ermittlerteam mit den Polizeiruf-Kommissaren zusammen (www.tvwiki.de/index.php/Tatort#Polzeiruf_110).

Episoden-Rezensionen der etwas anderen und lockeren Art findet man im Blog von Sopran (sopranisse.de/category/tatort/). Der Autor bloggt während der Tatort-Folgen im TV und kommentiert minutengenau zu Ereignissen in der Episode, die ihm erwähnenswert scheinen. Diese Vorgehensweise liefert ein ganz anderes Bild einer Episode, da der Blog-Eintrag mit dem Spannungsbogen entsteht.

Wer nach all dem immer noch nicht genug hat, kann sich zum Abschluss im Webangebot des Ersten den Klingelton der Titelmusik herunterladen und sich somit auch in der Tatort-freien Zeit von der einprägsamen Melodie berieseln lassen (www.daserste.de/tatort/beitrag_dyn~uid,3ohyn3d0eapt0n42~cm.asp). (ka)

### URLs auf einen Blick

www.daserste.de/tatort/

www.daserste.de/tatort/kommissare.asp

de.wikipedia.org/wiki/Harald_Krassnitzer

milch.junkies.ws/2007/05/20/revolution-beim-tatort-osterreich/

de.wikipedia.org/wiki/Tatort_(Fernsehreihe)#Liste_der_aktuellen_Tatort-Ermittler

www.tatort-fundus.de/web/index.php?id=3254

www.youtube.com/watch?v=veOJYxHlgW8

www.welt.de/fernsehen/article2026467/Die_bekanntesten_Augen_des_Tatorts.html

tatort-fans.de/tatort-001-taxi-nach-leipzig/

www.amazon.de/Taxi-nach-Leipzig-Sittengeschichte-Deutschlands/dp/393679147?ie=UTF8&s=books&qid=1211660082&sr=1-1

www.jstor.org/pss/488458

www.tatort-fundus.de/web/index.php?id=226

www.tvwiki.de/index.php/Tatort#Polzeiruf_110

sopranisse.de/category/tatort/

www.daserste.de/tatort/beitrag_dyn~uid,3ohyn3d0eapt0n42~cm.asp

Wer weitere URLs zum Thema kennt, hat die Möglichkeit, sie der Online-Version (www.heise.de/ix/artikel/2008/07/150/) hinzuzufügen.

# Vor 10 Jahren: Oben hui, unten naja

**Ein ursprünglich vor allem für islamische Länder geplantes Telefonieprojekt hat die hochfliegenden Pläne von Mitbewerbern wie Iridium überholt.**

Als vor wenigen Wochen die Erde in China bebte, druckte die „Süddeutsche“ als erste deutsche Tageszeitung einen Augenzeugenbericht von Klaus Därr ab. Die Redaktion hatte den deutschen Weltenbummler auf seinem Thuraya-Telefon erreicht, einem Gerät, das via Satellit kommuniziert, wenn keine Funkzelle auf der Erde vorhanden ist.

Die Idee, mit Satelliten eine Mobilkommunikation zu betreiben, die ohne „Schüsseln“ auskommt, ist nicht neu. In Ausgabe 7/98 meldete *iX*, dass Iridium die letzten fünf von insgesamt 66 Satelliten platzieren konnte und auf dem Weg zum Marktführer in diesem Segment sei.

Iridium war nicht allein auf weiter Flur. Damals wollte die Firma Teledesic (Hauptinvestor: Bill Gates) mit insgesamt 320 Satelliten in geringerer Höhe einen ähnlichen Service anbieten. Dank der geringen Flughöhe sollten die Mobiltelefone nicht so klobig ausfallen wie die Rufknochen von Iridium.

Weitere Player in dem Geschäft: die ebenfalls amerikanische ICO Global Communications, die mit wenigen Satelliten nur die USA abdecken wollten, und eben die Firma Thuraya aus Sarjah, die in den Vereinigten Arabischen Emiraten ein herkömmliches Mobilfunksystem errichtet hatte und zwei Satelliten über den Wüsten positionierte.

In ihren Geschäftsberichten fand sich eine merkwürdige Floskel: „Ziel ist es, alle Länder zu erreichen und zu vernetzen, in denen der Islam maßgeblich vertreten ist.“ Staaten wie Indonesien und Malaysia wollte man anschließen, aber auch die Wüstengebiete, weshalb Thuraya-Telefone von Anfang an mit GPS-Fähigkeiten konzeptioniert wurden. 20 arabische Investoren stellten dafür Geldmittel zur Verfügung, über deren Höhe bis heute spekuliert wird.

Zurück zu Iridium: Im September 1998 startete dieses Welttelefonnetz, in dem die Gesprächsminute 9,50 US-Dollar kostete. Iridium-Nutzer konnten von jedem Ort der Erde aus kommunizieren – nur nicht in Gebäuden. Während die Nutzer terrestrischer Mobilfunknetze mancherorts sogar in U-Bahnen telefonierten, standen die Iridium-Anhänger draußen im Regen. Den sich abzeichnenden Flop versuchten Iridium-Manager im Jahre 2000 zu verhindern, als sie mit Fluggesellschaften verhandelten, die Mobilfunk-Telefonie im Flieger anbieten wollten. Daneben bewarb man eine Datenflatrate mit 9600 Baud, während die Konkurrenz schon mit UMTS prahlte.

Die Iridium-Reste nutzt heute hauptsächlich die US-Armee – noch passabel im Vergleich zu Teledesic und ICO, die ebenfalls in Konkurs gingen und nur Weltraumschrott hinterließen. Geblieben und gediehen ist Thuraya, das nie den Anspruch hatte, ein weltumspannendes Netz zu errichten und lieber peu à peu erweiterte, unter anderem auch mit terrestrischen Funknetzen im Iran und Syrien. Erst Anfang 2008 wurden die Satelliten für die dritte Erweiterung des Netzes positioniert und sind seit April erreichbar. So kann jetzt in Indonesien via Thuraya telefoniert werden, aber auch in Japan und China.

*Detlef Borchers*

# MEHR KBYTES

## Internet

Anders als es einige Medien zum 15-jährigen Jubiläum des World Wide Web suggerierten, besteht das Internet aus mehr als dem WWW. E-Mail ist nach wie vor als Dinosaurier der Gattung Internet aktiv. Jüngere Sprösslinge sind Suchmaschinen und soziale Netze.

Wer suchet, Linklisten beliebigen Umfangs findet und nach der dritten Ergebnisseite noch weiterklickt, ist selbst schuld. Als nicht mehr ergooglebar gilt alles danach. Dass in Deutschland dies Suchen fast ausschließlich Googeln bedeutet, spricht ein bisschen gegen die freien Marktkräfte und viel für das Marketing von Google – inklusive der unprätentiösen Gestaltung der Suchseite.

Literatur zum Phänomen Google ist keine Erfindung dieses Jahres. Schon 2005 hat der Transcript-Verlag das von Kai Lehmann und Michael Schetsche herausgegebene „Die Google-Gesellschaft“ veröffentlicht. Im selben Jahr ist David Vises „Google Story“ erschienen. Jetzt hat Gerald Reischl für den österreichischen Ueberreuter-Verlag „Die Google Falle“ (mit Leerzeichen) geschrieben. Vom Titel her scheint die Lage an Dramatik gewonnen zu haben.

Reischl geht es um Google als Datensammler, als Wolf im Schafspelz: „Von Amerikanern erdacht, für Europäer gemacht“, heißt es auf Seite 150. Das bedeutet, dass die Dominanz des kalifornischen Suchmaschinenanbieters hier erheblich größer ist als im eigenen Land (circa 90 Prozent gegenüber etwa 60 Prozent). Umso wichtiger, dass Google-Nutzer – in der IT-Branche wahrscheinlich mehr als die genannten 90 Prozent – wissen, worauf sie sich einlassen.

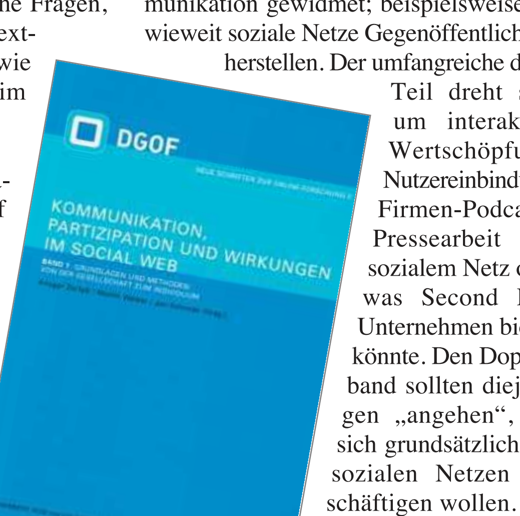
Eingängig geschrieben liest sich Reischls Warnung vor der „Datenkrake“, die mehr über Nutzer weiß als die Polizei, amüsant bis bedrohlich. Und die Aussicht, dass die Facebooks dieser Welt den Giganten irgendwann an Daten und Macht übertreffen könnten, erleichtert nicht unbedingt.

Im Mai vorigen Jahres fand in Berlin ein Symposium zu Suchmaschinen von morgen statt, aus dessen Beiträgen Friedemann Mattern als Herausgeber den bei acatech erschienenen Band „Wie arbeiten die Suchmaschinen von morgen?“ zusammengestellt hat. Darin beschreibt beispielsweise der KI-Forscher Wolfgang Wahlster, wie aus dem semantischen Web und dem Web 2.0 das Web 3.0 entstehen könnten: „Antwortmaschine“ heißt sein Gegenbegriff zur Suchmaschine von heute (Reischl streift das Thema ebenfalls: was Google in dieser Richtung unternimmt). Weitere Aspekte, die Aufsätze beleuchten, sind wirtschaftliche Fragen, was in die Volltextsuche gehört sowie was Suchen im Onlinegeschäft bedeutet.

An der Frage, ob wir auf dem Weg in die Google-Gesellschaft seien, kommt der Band naturgemäß nicht vorbei. Als Schnittstelle zur „informatisierten“ Welt haben Suchmaschinen große Bedeutung, der Umgang mit ihnen und das Leben in der genannten informatisierten Welt erfordern jedoch eine Kompetenz, die die schulische Ausbildung sicherlich (noch) nicht bietet. Geeignet für alle, die mehr als googeln wollen.

Kommunikation, die einst mündlich, später auch fernmündlich erfolgte, verlagert sich teilweise in Chat-Räume und soziale Netze. Das kümmert die Wissenschaft, in diesem Falle die Deutsche Gesellschaft für Online-Forschung. Ansgar Zerfaß, Martin Welker und Jan Schmidt haben beim Herbert-von-Halem-Verlag in einer von der DGOF herausgegebenen Reihe zwei Bände zu „Kommunikation, Partizipation und Wirkungen im Social Web“ betreut, die unterschiedliche Aspekte der sozialen Netze analysieren.

Im ersten Band widmen die Autoren sich Konzepten und Anwendungen. Von Wikis, Blogs und rechtlicher Verantwortung im sozialen Netz ist hier ebenso die Rede wie von Podcasts, Privatheit und Chancen für die Sozialforschung. Der zweite Band verlässt den prinzipiellen und „privaten“ Rahmen, indem er Beiträge versammelt, die unterschiedliche „Strategien und Anwendungen“ aus Unternehmenssicht behandeln. Wie Journalisten in der Blogosphäre recherchieren und über welche Blogs sie berichten. Mehrere Aufsätze sind der politischen Kommunikation gewidmet; beispielsweise inwieweit soziale Netze Gegenöffentlichkeit herstellen. Der umfangreiche dritte Teil dreht sich um interaktive Wertschöpfung: Nutzereinbindung, Firmen-Podcasts, Pressearbeit mit sozialem Netz oder was Second Life Unternehmen bieten könnte. Den Doppelband sollten diejenigen „angehen“, die sich grundsätzlich mit sozialen Netzen beschäftigen wollen.




Webmaster wollen bei Suchmaschinen in der Rangfolge oben stehen, vorzugsweise auf der ersten Seite. Darauf müssen sie ihre Seiten ausrichten, wenn das Publikum sie finden soll. Daniel Koch hat im vorigen Jahr mit „Suchmaschinen-Optimierung“ eine Anleitung für Rat suchende Webmaster geschrieben, verlegt von Addison-Wesley. Außer der Verbesserung des HTML-Quellcodes kommen Flash, PDF und Marketing zu ihrem Recht.

Abseits von Suchmaschinen und Blogs hat ein anderer Trend zugelegt: Telefonieren über IP. Gerd Flaig und seine Koautoren haben bei der Open Source Press in diesem Jahr die zweite Auflage ihres „Internet-Telefonie“ veröffentlicht, das außer Aktualisierungen ein zusätzliches praktisches Kapitel enthält.

*Henning Behme*

Gerd Flaig, Martin Hoffmann, Siggi Langauf, Stefan Tichy; **Internet-Telefonie**; VoIP mit Asterisk und SER; München (Open Source Press) 2008; 2., aktualisierte und erweiterte Auflage; 576 Seiten; € 39,90 (Paperback)

Daniel Koch; **Suchmaschinen-Optimierung**; Webseiten-Marketing für Entwickler; München (Addison-Wesley) 2007; 351 Seiten; € 29,95 (Paperback)

Friedemann Mattern (Hrsg.); **Wie arbeiten die Suchmaschinen von morgen?**; Informationstechnische, politische und ökonomische Perspektiven; München (acatech) 2008; 140 Seiten; € 22,– (Paperback) oder PDF

Gerald Reischl; **Die Google Falle**; Die unkontrollierte Weltmacht im Internet; Wien (Ueberreuter) 2008; 190 Seiten; € 19,95 (gebunden)

Ansgar Zerfaß, Martin Welker, Jan Schmidt (Hrsg.); **Kommunikation, Partizipation und Wirkungen im Social Web**; Köln (Herbert von Halem) 2008; zwei Bände; 397/493 Seiten; € 27,50/29,50 (Paperback)




Christian Bauer, Gavin King

## Java Persistence mit Hibernate

München, Wien 2007
Carl Hanser Verlag
Übersetzt von Jürgen Dubau
729 Seiten
59,90 €
ISBN 978-3-446-40941-5

Java-Objekte in einer relationalen Datenbank auf der Basis objektrelationaler Abbildung (object-relational mapping, ORM) zu speichern hat in den letzten Jahren an Bedeutung gewonnen. Zahlreiche Klassenbibliotheken beschäftigen sich damit, und seit dem Erscheinen der Java Enterprise Edition 5 (JEE5) liegt in Form der Java Persistence API (JPA) sogar eine standardisierte API vor. In vielen Punkten Pate gestanden bei der Ausarbeitung des JPA-Standards hat das Persistenz-Framework Hibernate, das eine eigene, proprietäre API sowie JPA unterstützt.

Es überrascht daher nicht, dass sich zahlreiche Parallelen bei der Nutzung dieser beiden Alternativen finden. Dennoch ist die Hibernate-API nicht gleichzusetzen mit der JPA, wie „Java Persistence mit Hibernate“ verdeutlicht. Gemeinsamkeiten von Hibernate und JPA und Unterschiede, die längst nicht nur syntaktischer Natur sind, arbeiten die Autoren anhand heraus.

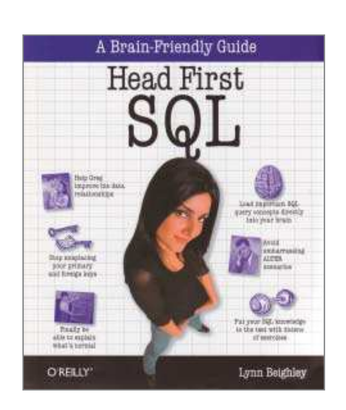
Gleich mehrere Kapitel beschäftigen sich mit der Abbildung von Vererbung, Collections und Entity-Assoziationen durch Quelltext-Annotationen oder XML-Mapping-Dateien. Ebenfalls ausführlich kommen gleichzeitige Datenzugriffe, Transaktionen und Konversationen zur Sprache. Die Optimierung von Anwendungen bildet einen weiteren Themen-Schwerpunkt. Das Wissen um Fetching- und Caching-Strategien sowie deren Beeinflussung hilft bei der Vermeidung von Performance-Engpässen.

Sofern sich durch die Benutzung der nativen Hibernate-API Vorteile gegenüber der JPA ergeben, stellen die Autoren geeignete Erweiterungen von Hibernate vor. Diese lassen sich nicht nur für eine verbesserte Optimierung, sondern außerdem bei der Abbildung von Legacy-Datenbank-Systemen auf Java-Objekte nutzen. Ein abschließendes Kapitel beschäftigt sich mit dem Einsatz von ORM in mehrschichtigen Anwendungen.

Gleichgültig, ob man die Hibernate-API einsetzt, sich auf die JPA konzentriert oder eine Kombination beider in Betracht zieht: Nach der Lektüre ist man für ihren Einsatz gewappnet. Am Ende jedes Kapitels werden wichtige Eigenschaften beider APIs gegenübergestellt. Das Buch, das sich registrierte Käufer kostenlos herunterladen können, ist gut zu lesen – das spricht für die Übersetzung. Da lassen sich sogar unbeabsichtigte Buchstabendreher (Tippgicht) im Text verschmerzen.

UWE SEIMET






Lynn Beighley

## Head First SQL

Sebastopol, CA 2007
O'Reilly Media
607 Seiten
43,– €
ISBN 978-0-596-52684-9

Lynn Beighley nimmt den Leser in „Head First SQL“ mit auf eine Reise durch die Welt der relationalen Datenbanken. In dieser Welt spricht man SQL, und diese Anfragesprache lernt der Leser auf die bekannte lockere Art und Weise der Reihe.

Die Reise beginnt mit dem Kapitel „A place for everything“, einer Motivation der Datenbankthematik im Allgemeinen und den Grundlagen der relationalen Datenbanken im Besonderen. Die folgenden beiden Kapitel führen den Leser an die DML-Konstrukte (Data Manipulation Language) *INSERT*, *SELECT*, *UPDATE* und *DELETE* von SQL heran. Anschließend stellt Beighley die Frage „Why be normal?“ und widmet sich mit einigen „fishy tables“ (zu übersetzen als „Tabellen, mit denen etwas faul ist“) den Normalformen von Tabellen.

„Rewriting the past“ komplettiert die Liste der DDL-Konstrukte von SQL mit dem *ALTER*-Statement. Kapitel 6 bis 10 vertiefen das Wissen über die Formulierung von Anfragen. Die fängt mit Aggregatfunktionen wie *ORDER BY* und *GROUP BY* sowie *AVG*, *MIN*, *MAX* oder *SUM* an und führt über einfache Joins und Unterabfragen zu Outer Joins, Self-Joins und Unions. Kapitel 11 zeigt dem Leser, dass zu viele Köche den Brei verderben und wie man die Schwierigkeiten, die durch den gleichzeitigen lesenden und schreibenden Zugriff mehrerer Benutzer auf dieselbe Datenbank entstehen, mit Transaktionen, Constraints und Views in den Griff bekommt. Die Zugriffssicherheit von Datenbanken ist Thema des letzten Kapitels. Die nun folgenden Anhänge widmen sich unter anderem den zuvor nicht behandelten Top-10-Themen, die aber zumindest ansatzweise vorkommen sollen. Hierzu gehört beispielsweise die Nutzung einer relationalen Datenbank aus einer Programmiersprache wie PHP heraus. Informationen zu Installation und Konfiguration von MySQL sowie eine Werkzeugübersicht sind ebenfalls in den Anhängen zu finden.

Lynn Beighley ist es gelungen, dieses sonst recht theoretisch und trocken vermittelte Thema interessant und locker, aber dennoch anspruchsvoll zu präsentieren. Alle wesentlichen Konzepte relationaler Datenbanken und Aspekte der damit verbundenen Anfragesprache SQL behandelt sie – sogar diejenigen, die sonst „wehtun“ (Stichwort: nicht korrelierte Unterabfragen). Die zahlreichen Codebeispiele lassen sich mit MySQL einfach und schnell nachvollziehen.

SEBASTIAN BERGMANN

---




Wolf Schneider

## Speak German

**Warum Deutsch manchmal besser ist**

Hamburg 2008
Rowohlt Verlag
191 Seiten
14,90 €
ISBN 978-3-498-06393-1

Ungewöhnlich gut unterrichtete Kreise berichten immer wieder von überlebenden Siemensianern, die noch heute von der „Wagenrücklauftaste“ sprechen. Sage deshalb niemand, keiner pflege die deutsche Sprache mehr. Dass viele ihr den Rücken kehren, wenn es um die Steigerung des eigenen Rufs durch Berufsbezeichnung oder den Nachweis der Englischkompetenz geht, steht auf einem anderen Blatt.

Deshalb kümmert sich Wolf Schneider, der diverse Bücher zum Deutschen geschrieben hat, in seinem neuen Band häufig um Begriffe, die mit der IT (gesprochen: ei-tie) zusammenhängen. Mit „Speak German“ hat er eine Art Bestandsaufnahme der Überfremdung vorgelegt, ohne tümeln zu wollen. Gründe genug dafür enthält insbesondere das Computerdeutsch, allenfalls vom Jargon der Werbebranche übertroffen. Vom Kick-off Event zu gedownloadet und vom Notebook bis zur fast schon ewig deutsch klingenden Technologie reicht die Palette.

Schneider gehört zu den Gründern der Aktion Lebendiges Deutsch, die sich innerhalb der Stiftung Deutsche Sprache bemüht, jeden Monat ein deutsches Wort für ein englisches zu finden (jeder kann per Mail oder Brief eigene Vorschläge einreichen) und vielleicht sogar durchzusetzen. Darunter sind immer wieder Wörter, die der Computerei entstammen, allerdings sträuben sich bei manchen Übertragungen die letzten Haare. Der Klapprechner dürfte ebenso chancenlos sein wie der Blinker. Anderes koexistiert seit geraumer Zeit: Computer und Rechner, Homepage und Startseite. Flatrate klingt moderner als Pauschale, und die Website (die besser „der“ heißen sollte) könnte gleich mehrere Entsprechungen haben, die gelegentlich sogar zu lesen sind: Netzauftritt, Internetauftritt/-präsenz.

Dass Eindeutschungsversuche von Erfolg gekrönt sein können, hat die Geschichte bewiesen (und Schneider referiert es). Von Zeesen im 17. und Campe im 19. Jahrhundert haben eine Reihe deutscher Begriffe durchsetzen können: Schauspieler statt Acteur oder Schlafwagen statt Dormeuse. Bismarck hat 1874 760 Eindeutschungen verfügt (Briefumschlag, Postkarte). In vielen Fällen haben sich allerdings beide Wörter gehalten (etwa Augenblick/Moment).

Schneider hat viele Details zusammengetragen: beispielsweise warum Firmen ihre englischen Werbesprüche der Neunzigerjahre nicht mehr verwenden. Einziges Manko: Zwar stellt Schneider Organisationen und Initiativen vor, aber nicht einmal die von ihm mitbegründete Aktion Lebendiges Deutsch würdigt er einer URL. Deshalb hier der Hinweis auf www.aktionlebendigesdeutsch.de. Dort befindet sich unter anderem ein Archiv bislang übersetzter Begriffe.

Insgesamt eine kurzweilige Lektüre, die Leser zwischen Grinsen über andere und sich selbst schwanken lassen kann.

HENNING BEHME



MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

Postfach 61 04 07, 30604 Hannover; Helstorfer Straße 7, 30625 Hannover

**Redaktion**
Telefon: 05 11/53 52-387, Fax: 05 11/53 52-361, E-Mail: post@ix.de
Abonnements: Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

**Herausgeber:** Christian Heise, Ansgar Heise

**Redaktion:** Chefredakteur: Jürgen Seeger (JS) -386

Stellv. Chefredakteur: Henning Behme (hb) -374

Ltd. Redakt.: Kersten Auel (ka) -367, Ralph Hülsenbusch (rh) -373, Bert Ungerer (un) -368

Jürgen Diercks (jd) -379, Christian Kirsch (ck) -590, Wolfgang Möhle (WM) -384, Susanne Nolte (sun) -689, André von Raison (avr) -377, Michael Riepe (mr) -787, Ute Roos (ur) -535

Redaktionsassistenz: Carmen Lehmann (cle) -387, Michael Mentzel (mm) -153

**Korrespondent Köln/Düsseldorf/Ruhrgebiet:**
Achim Born, Siebengebirgsallee 82, 50939 Köln,Telefon: 02 21/4 20 02 62,
E-Mail: ab@ix.de

**Korrespondentin München:**
Susanne Franke, Ansbacherstr. 2, 80796 München, Telefon: 089/28 80 74 80,
E-Mail: sf@ix.de

**Ständige Mitarbeiter:** Torsten Beyer, Detlef Borchers, Fred Hantelmann, Kai König, Michael Kuschke, Barbara Lange, Stefan Mintert, Holger Schwichtenberg, Susanne Schwonbeck, Christian Segor, Diane Sieger, Axel Wilzopolski, Nikolai Zotow

**DTP-Produktion:** Enrico Eisert, Wiebke Preuß, Matthias Timm, Hinstorff Verlag, Rostock

**Korrektorat/Chefin vom Dienst:** Anja Fischer

**Fotografie:** Martin Klauss Fotografie, Despetal/Barfelde

Titelidee: ***iX;*** Titel- und Aufmachergestaltung: Dietmar Jokisch

**Verlag und Anzeigenverwaltung:**
Heise Zeitschriften Verlag GmbH & Co. KG, Postfach 61 04 07, 30604 Hannover;
Helstorfer Straße 7, 30625 Hannover; Telefon: 05 11/53 52-0, Fax: 05 11/53 52-129

**Geschäftsführer:** Ansgar Heise, Steven P. Steinkraus, Dr. Alfons Schräder

**Mitglied der Geschäftsleitung:** Beate Gerold

**Verlagsleiter:** Dr. Alfons Schräder

**Anzeigenleitung:** Michael Hanke -167, E-Mail: michael.hanke@heise.de

**Assistenz:** Christine Richter -534, E-Mail: christine.richter@heise.de

**Anzeigendisposition:** Christine Richter -534, E-Mail: christine.richter@heise.de

**Anzeigenverkauf:** PLZ-Gebiete 0–3, Ausland:
Oliver Kühn -395, E-Mail: oliver.kuehn@heise.de,
PLZ-Gebiete 8–9: Ralf Räuber -218, E-Mail: ralf.raeuber@heise.de
Sonderprojekte: Isabelle Paeseler -205, E-Mail: isabelle.paeseler@heise.de

**Anzeigen-Inlandsvertretung:** PLZ-Gebiete 4–7:
Karl-Heinz Kremer GmbH, Sonnenstraße 2, D-66957 Hilst,
Telefon: 063 35/92 17-0, Fax: 063 35/92 17-22, E-Mail: karlheinz.kremer@heise.de

**Anzeigen-Auslandsvertretung:**
**Großbritannien, Irland:** Oliver Smith & Partners Ltd. Colin Smith, 18 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX, UK, Telefon: (00 44) 20/79 78-14 40, Fax: (00 44) 20/79 78-15 50,
E-Mail: colin@osp-uk.com

**Anzeigenpreise:** Es gilt die Anzeigenpreisliste Nr. 20 vom 1. Januar 2008.

**Leiter Vertrieb und Marketing:** Mark A. Cano (-299)

**Werbeleitung:** Julia Conrades (-156)

**Teamleitung Herstellung:** Bianca Nagel (-456)

**CD-Herstellung:** Klaus Ditze (Ltg.), Nicole Tiemann

**Druck:** Dierichs Druck + Media GmbH & Co. KG, Kassel

**Sonderdruck-Service:** Bianca Nagel (-456, Fax: -360)

**Verantwortlich:** Textteil: Jürgen Seeger; Anzeigenteil: Michael Hanke

***iX* erscheint monatlich**

Einzelpreis € 5,50, Österreich € 6,20, Schweiz CHF 10,70, Benelux € 6,70, Italien € 6,70

Das Abonnement für 12 Ausgaben kostet: Inland € 56,–, Ausland (außer Schweiz) € 63,–;
Studentenabonnement: Inland € 42,–, Ausland (außer Schweiz) € 47,– nur gegen Vorlage der Studienbescheinigung (inkl. Versandkosten Inland € 8,30, Ausland € 13,30), Luftpost auf Anfrage.

*iX-Abo+* (inkl. jährlicher Archiv-CD-ROM) jeweils zzgl. € 8,–

Für GI-, VDI-KfIT-, GUUG-, IUG-, LUG-, AUGE- und Mac-e.V.-Mitglieder gilt der Preis des Studentenabonnements (gegen Mitgliedsausweis).

**Kundenkonto in Österreich:**
Dresdner Bank AG, BLZ 19675, Kto.-Nr. 2001-226-00 EUR, SWIFT: DRES AT WX

**Kundenkonto in der Schweiz:** UBS AG, Zürich, Kto.-Nr. 206 P0-465.060.0

**Abo-Service:**
Heise Zeitschriften Verlag, Kundenservice, Postfach 810520, 70522 Stuttgart,
Telefon: 0711/72 52-292, Fax: 0711/72 52-392, E-Mail: abo@heise.de

**Für Abonnenten in der Schweiz Bestellung über:**
Thali AG, Aboservice, Industriestr. 14, CH-6285 Hitzkirch,
Telefon: 041/919 66 11, Fax: 041/919 66 77, E-Mail: abo@thali.ch, Internet: www.thali.ch (Jahresabonnement: CHF 111,–; Studentenabonnement: CHF 83,25)

Das Abonnement ohne Archiv-CD-ROM ist jederzeit mit Wirkung zur jeweils übernächsten Ausgabe kündbar. Das *iX-Abo+* (incl. jährlicher Archiv-CD-ROM) gilt zunächst für ein Jahr und ist danach zur jeweils übernächsten Ausgabe kündbar.

**Vertrieb Einzelverkauf** (auch für Österreich, Luxemburg und Schweiz): MZV Moderner Zeitschriften Vertrieb GmbH & Co. KG, Breslauer Str. 5, 85386 Eching, Telefon: 089/319 06-0,
Fax: 089/319 06-113, E-Mail: mzv@mzv.de, Internet: www.mzv.de



**ISSN 0935-9680**







## Acht Web Application Firewalls

Schwachstellen in Webanwendungen können die IT-Infrastruktur eines Unternehmens gefährden. Helfen sollen sogenannte WAFs: Web Application Firewalls, die die Kommunikation auf Anwendungsebene (HTTP/HTTPS) analysieren. Dabei inspizieren sie im Detail die Anfragen an den Webserver sowie dessen Antworten an den Webclient. Ein Vergleich von acht WAFs.

## Programme aus Modellen

Der große Traum vieler Softwareentwickler: die weitgehende Automatisierung der lästigen manuellen Kodierung. Vielversprechende Ansätze liefert die modellgetriebene Softwareentwicklung. Auch im Umfeld freier Software findet man etliche geeignete Werkzeuge. Dazu gehören der Java Application Builder jABC ebenso wie die Generator-Frameworks AndroMDA und openArchitectureWare.

**Heft 08/2008 erscheint am 24. Juli 2008**
Änderungen vorbehalten

## Neues Tutorial: Rich Clients mit Silverlight

Nachdem Microsoft im letzten Jahr die ersten Betaversionen von Silverlight – seiner Alternative zum Flash-Plug-in – präsentiert hat, steht jetzt die Version 2 mit etlichen Neuerungen ins Haus. Ein dreiteiliges Tutorial zeigt, wie sich mit der plattform- und browserunabhängigen Version des .Net Framework auf XAML-Basis Webanwendungen entwickeln lassen.

## AMDs Quadcore vom TLB-Fehler befreit

Nachdem es AMD endlich gelungen ist, seinen im vorigen Jahr unter dem Projektnamen „Barcelona“ propagierten Quad-Core-Prozessor vom Fehler im Translation Look-aside Buffer zu befreien, konnten die ersten Hersteller ihre neuen Server mit AMDs Opteron-CPUs auf den Markt bringen. Zum Test kam ein nur eine Einbaueinheit hohes Rack-Mount-System von CPI mit vier Prozessorchips, in dem somit insgesamt 16 CPU-Kerne auf Arbeit warten. Im *iX*-Labor mussten sie sich unter hohen Lasten bewähren.

## Neues MAC-System für Linux

Bislang gibt es für Linux mit SELinux und AppArmor zwei Mandatory-Access-Control-Systeme (MAC) im Standard-Kernel. Ersteres steht im Ruf, zu kompliziert zu sein. Pfadbasierende Systeme wie AppArmor gelten als nicht sicher genug. Mit SMACK – dem Simple Mandatory Access Control Kernel – hat innerhalb nur eines Jahres ein weiterer Vertreter der Gattung den Sprung in den Default-Kernel geschafft. Er ist wie SELinux Label-basiert, kommt aber ohne komplexe Konfiguration aus.



**Das bringen**






**Notebooks aufrüsten:** Was geht, wie man’s macht

**Profi-NAS:** Rack-tauglicher Netzwerkspeicher

**Überall online:** Web-Kontakt auf Reisen

**Multitouch:** Mehrfingerbetrieb auf Touchscreens

**c't 14/08 ab 23. Juni im Handel**






**Die gedopte Elite:** Mit Medikamentenhilfe zu Höchstleistungen

**GPS für alle:** Neues Konzept für die stromsparende Lokalisierung

**Bits und Gene:** Bioinformatik als wichtigstes Werkzeug der Medizin

**TR 7/08 jetzt am Kiosk**

TELEPOLIS
MAGAZIN DER NETZKULTUR



**Peter Bürger:** AOK: „Alle Oder Keiner“ – Notizen aus dem Krankentagebuch eines Freiberuflers

**Hans Schmid:** Der Elvis des Massenmords – Charles Manson und die Tate-LaBianca-Morde

**www.heise.de/tp/**